Risk Assessment Report

Executive Summary

1. Introduction

In order to supplement the Risk Assessment Report (Getir, 2023) provided earlier and to help better visualise the potential impact of pre-digitalisation and post-digitalisation threats, an Attack Tree Generator application was developed in Python. Once the application is tested and verified, the application was used to generate attack trees for the Pampered Pets business. The assessment was concluded with the comparison of attack trees of both scenarios (pre- and post-digitalisation) and drawing conclusions.

2. Attack Tree Generator Application

The Attack Tree Application is a python application which accepts a .json document containing attack tree data and generates an attack tree out of it.

2.1. Features

The application has the following features:

- Generates a CLI-based attack tree from a .json file.
- Calculates the overall risk rating based on the risk values provided by the user.
- Generates a visual attack tree with risk values for each leaf node and leaf and exports it to a .png file.
- Generates partial attack trees starting from a chosen leaf node.
- Allows for entering/changing risk values for leaves to analyse the impact of different scenarios.

2.2. Usage

To make use of the application, follow the steps below:

- Prepare a .json document which contains the attack tree data. You can use the template (data.json) in the data folder of the application.
- Start the application by running the following command in the terminal:

```
python3 tree_generator.py
```

- Load the .json file to memory.
- Generate a CLI-based attack tree to see the current state of the tree and check if the data in the .json file appears as expected.
- Calculate the risk rating for leaf nodes as well as the overall risk rating for the attack tree.
- Generate a visual attack tree in .png format.

Please refer to the application readme file for detailed explanation of the usage and features of the application.

3. Methodology

3.1. Customized Quantitative Threat Modelling Method (QTTM)

Quantitative Threat Modelling Method (QTTM) (Potteiger et al., 2016) was adopted and customized to build on the previous risk assessment. QTTM suggests building component attack trees based on the categories of STRIDE (Microsoft, 2022) and calculating risk scores using CVSS (FIRST, 2023).

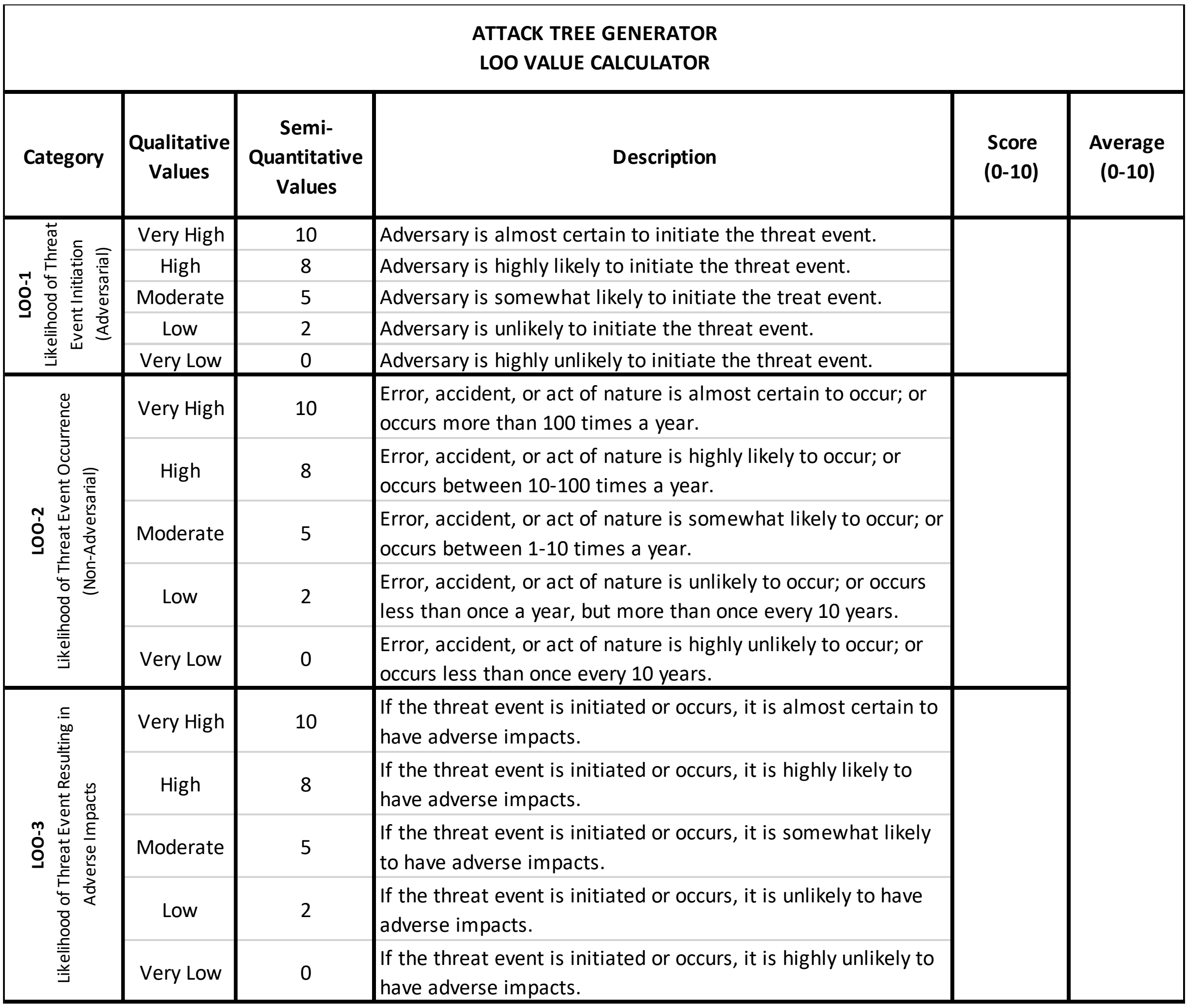
However, for this particular assessment, it was decided to use the Likelihood of Occurrence scores suggested by NIST (2012) instead of CVSS, because thanks to its simplicity, it doesn’t require any knowledge or experience about risk assessment, and anyone can use it easily.

3.2. Calculation of Likelihood of Occurrence (LOO)

The NIST (2012) suggest risk management professionals to assess the likelihood of occurrence of threat events from three different aspects and goes on to provide a separate assessment scale for each of them:

- Likelihood of threat event initiation (adversarial)
- Likelihood of threat event occurrence (non-adversarial)
- Likelihood of threat event resulting in adverse impacts

For simpler use, these three assessment scales were combined into one which produces a value on a scale of 0-10 to populate the risk values of the leaves in the Attack Tree Generator application:



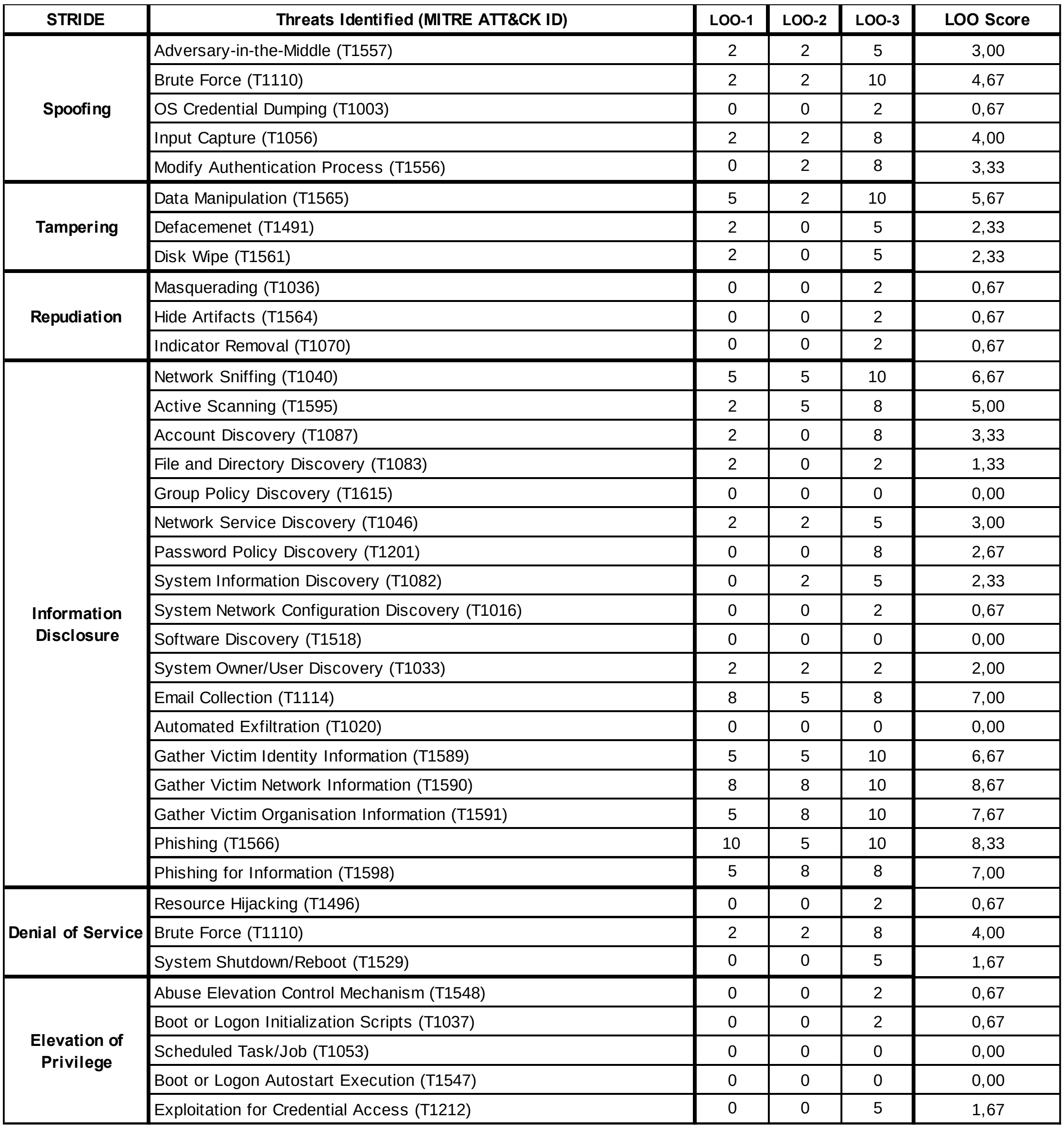
ATTACK TREE GENERATOR
LOO VALUE CALCULATOR

Category	Qualitative Values	Semi-Quantitative Values	Description	Score (0-10)	Average (0-10)
LOO-1 Likelihood of Threat Event Initiation (Adversarial)	Very High	10	Adversary is almost certain to initiate the threat event.		
	High	8	Adversary is highly likely to initiate the threat event.		
	Moderate	5	Adversary is somewhat likely to initiate the treat event.		
	Low	2	Adversary is unlikely to initiate the threat event.		
	Very Low	0	Adversary is highly unlikely to initiate the threat event.		
LOO-2 Likelihood of Threat Event Occurrence (Non-Adversarial)	Very High	10	Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.		
	High	8	Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.		
	Moderate	5	Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.		
	Low	2	Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.		
	Very Low	0	Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.		
LOO-3 Likelihood of Threat Event Resulting in Adverse Impacts	Very High	10	If the threat event is initiated or occurs, it is almost certain to have adverse impacts.		
	High	8	If the threat event is initiated or occurs, it is highly likely to have adverse impacts.		
	Moderate	5	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.		
	Low	2	If the threat event is initiated or occurs, it is unlikely to have adverse impacts.		
	Very Low	0	If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.		

In order to facilitate risk score calculation, an automated LOO calculator was prepared and offered for free use here (copy and use): http://bit.ly/loo-calculator

Using this calculator, the following LOO values were calculated for each of the threats identified in the previous report:

3.2.1 LOO values for pre-digitalisation



STRIDE	Threats Identified (MITRE ATT&CK ID)	LOO-1	LOO-2	LOO-3	LOO Score
Spoofing	Adversary-in-the-Middle (T1557)	2	2	5	3,00
	Brute Force (T1110)	2	2	10	4,67
	OS Credential Dumping (T1003)	0	0	2	0,67
	Input Capture (T1056)	2	2	8	4,00
	Modify Authentication Process (T1556)	0	2	8	3,33
Tampering	Data Manipulation (T1565)	5	2	10	5,67
	Defacemenet (T1491)	2	0	5	2,33
	Disk Wipe (T1561)	2	0	5	2,33
Repudiation	Masquerading (T1036)	0	0	2	0,67
	Hide Artifacts (T1564)	0	0	2	0,67
	Indicator Removal (T1070)	0	0	2	0,67
Information Disclosure	Network Sniffing (T1040)	5	5	10	6,67
	Active Scanning (T1595)	2	5	8	5,00
	Account Discovery (T1087)	2	0	8	3,33
	File and Directory Discovery (T1083)	2	0	2	1,33
	Group Policy Discovery (T1615)	0	0	0	0,00
	Network Service Discovery (T1046)	2	2	5	3,00
	Password Policy Discovery (T1201)	0	0	8	2,67
	System Information Discovery (T1082)	0	2	5	2,33
	System Network Configuration Discovery (T1016)	0	0	2	0,67
	Software Discovery (T1518)	0	0	0	0,00
	System Owner/User Discovery (T1033)	2	2	2	2,00
	Email Collection (T1114)	8	5	8	7,00
	Automated Exfiltration (T1020)	0	0	0	0,00
	Gather Victim Identity Information (T1589)	5	5	10	6,67
	Gather Victim Network Information (T1590)	8	8	10	8,67
	Gather Victim Organisation Information (T1591)	5	8	10	7,67
	Phishing (T1566)	10	5	10	8,33
	Phishing for Information (T1598)	5	8	8	7,00
Denial of Service	Resource Hijacking (T1496)	0	0	2	0,67
	Brute Force (T1110)	2	2	8	4,00
	System Shutdown/Reboot (T1529)	0	0	5	1,67
Elevation of Privilege	Abuse Elevation Control Mechanism (T1548)	0	0	2	0,67
	Boot or Logon Initialization Scripts (T1037)	0	0	2	0,67
	Scheduled Task/Job (T1053)	0	0	0	0,00
	Boot or Logon Autostart Execution (T1547)	0	0	0	0,00
	Exploitation for Credential Access (T1212)	0	0	5	1,67

3.2.2. LOO values for post-digitalisation

STRIDE	Threats Identified (MITRE ATT&CK ID)	LOO-1	LOO-2	LOO-3	LOO Score
Spoofing	Adversary-in-the-Middle (T1557)	5	5	5	5,00
	Brute Force (T1110)	8	5	8	7,00
	OS Credential Dumping (T1003)	2	0	5	2,33
	Input Capture (T1056)	2	5	8	5,00
	Modify Authentication Process (T1556)	2	2	5	3,00
	Exploit Public-Facing Application (T1190)	0	2	0	0,67
	Forge Web Credentials (T1606)	2	5	8	5,00
	Steal Web Session Cookie (T1539)	0	2	2	1,33
	Compromise Accounts (T1586)	2	2	8	4,00
Tampering	Data Manipulation (T1565)	5	5	10	6,67
	Defacemenet (T1491)	0	0	5	1,67
	Account Manipulation (T1098)	2	5	10	5,67
	Modify Cloud Compute Infrastructure (T1578)	0	0	10	3,33
	Disk Wipe (T1561)	0	2	10	4,00
Repudiation	Masquerading (T1036)	2	0	2	1,33
	Hide Artifacts (T1564)	0	0	2	0,67
	Indicator Removal (T1070)	2	0	5	2,33
Information Disclosure	Network Sniffing (T1040)	8	10	8	8,67
	Active Scanning (T1595)	10	10	8	9,33
	Account Discovery (T1087)	5	8	8	7,00
	File and Directory Discovery (T1083)	2	2	5	3,00
	Group Policy Discovery (T1615)	5	2	5	4,00
	Network Service Discovery (T1046)	5	5	5	5,00
	Password Policy Discovery (T1201)	8	8	10	8,67
	System Information Discovery (T1082)	8	8	8	8,00
	System Network Configuration Discovery (T1016)	8	8	5	7,00
	Software Discovery (T1518)	2	2	5	3,00
	System Owner/User Discovery (T1033)	5	5	5	5,00
	Cloud Infrastructure Discovery (T1580)	5	8	5	6,00
	Cloud Service Dashboard (T1538)	10	8	10	9,33
	Cloud Service Discovery (T1526)	5	5	8	6,00
	Cloud Storage Object Discovery (T1619)	8	8	10	8,67
	Credentials from Password Stores (T1555)	8	0	8	5,33
	Unsecured Credentials (T1552)	10	10	10	10,00
	Email Collection (T1114)	8	8	8	8,00
	Automatred Exfiltration (T1020)	2	0	5	2,33
	Gather Victim Identity Information (T1589)	8	5	10	7,67
	Gather Victim Network Information (T1590)	8	5	10	7,67
	Gather Victim Organisation Information (T1591)	5	2	8	5,00
	Search Open Technical Databases (T1596)	5	5	2	4,00
	Search Open Websites/Domains (T1593)	5	5	5	5,00
	Search Closed Sources (T1597)	2	2	2	2,00
	Search Victim-Owned Websites (T1594)	5	2	5	4,00
	Transfer Data to Cloud Account (T1537)	5	0	5	3,33
	Phishing (T1566)	10	10	10	10,00
	Phishing for Information (T1598)	10	10	10	10,00
Denial of Service	Resource Hijacking (T1496)	2	0	0	0,67
	Unused/Unsupported Cloud Regions (T1535)	0	0	0	0,00
	Network Denial of Service (T1498)	8	8	10	8,67
	Endpoint Denial of Service (T1499)	5	5	10	6,67
	Brute Force (T1110)	8	8	5	7,00
	System Shutdown/Reboot (T1529)	2	0	5	2,33
Elevation of Privilege	Abuse Elevation Control Mechanism (T1548)	0	0	2	0,67
	Boot or Logon Initialization Scripts (T1037)	0	0	2	0,67
	Scheduled Task/Job (T1053)	0	0	2	0,67
	Boot or Logon Autostart Execution (T1547)	0	0	2	0,67
	Valid Accounts (T1078)	8	5	10	7,67
	Create Account (T1136)	5	8	8	7,00
	Exploitation for Credential Access (T1212)	5	2	5	4,00

3.3. Attack tree

As the final step, the attack tree was designed based on STRIDE threat categories, in accordance with the QTTM. When attack tree is generated, an overall risk score is calculated based on the LOO values of the leaves.

In order generate attack trees for the current state of Pampered Pets as well as for the post-digitalisation scenario, two different .json files were prepared. The .json files with the attack tree data for both scenarios can be found in the appendices. For convenience, four different .json files are provided:

- Pre-digitalisation attack tree data
- Pre-digitalisation attack tree data - short
- Post-digitalisation attack tree data
- Post-digitalisation attack tree data - short

It is recommended to use the .json files named "-short" IDs when there is a space restriction because instead of full threat names, only MITRE ATT&CK library IDs were used to save space. Otherwise, the file with the full threat names may prove to be more informative, even though resulting attack trees may be much larger.

These files can be used to feed the attack tree generator application to generate the trees and to analyse different scenarios by changing the LOO values for leaves. The files are included in the "/data" folder, so they can be used simply by loading them to the memory.

3.4. Risk rating

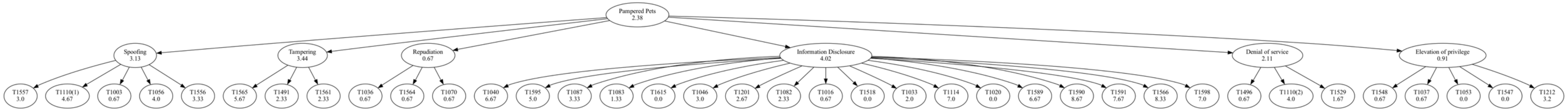
Based on the overall risk score that is calculated, the overall risk rating of the system is determined based on the scale below, which is also derived from NIST's recommendation (2012):

Risk Rating	Evaluation
10.0 – 9.51	Very High
9.50 – 7.91	High
7.90 – 2.01	Moderate
2.0 – 0.51	Low
0.50 – 0	Very Low

4. Results and Discussion

Using the scores calculated and the attack tree data provided, the pre-digitalisation and post-digitalisation attack trees were generated and the overall risk rating for both scenarios were calculated as below. Only MITRE ATT&CK library technique IDs are used for leaves in order to save space, full names of the threats identified can be found out from the LOO calculation tables above.

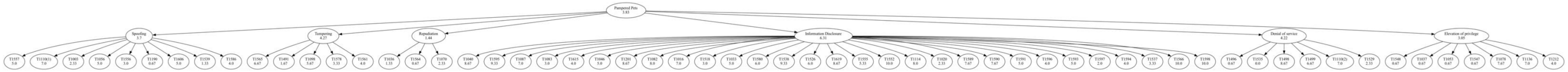
4.2. Pre-digitalisation attack tree:



Overall risk score: 2.38

Overall risk rating: Moderate

4.3. Post-digitalisation attack tree:



Overall risk score: 3.83

Overall risk rating: Moderate

4.4. Discussion of the results:

As it can be clearly seen from the attack trees and the overall risk scores above, digitalisation of the business increases the overall risk score significantly (from 2.38 to 3.83). The larger attack tree also indicates that the digitalisation leads to a larger attack surface.

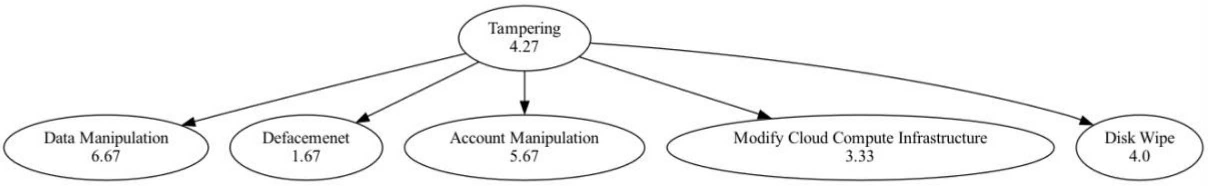
However, even though the increase in the risk score, the risk rating remains the same in both scenarios as “Moderate”. It is assessed that the findings are in line with the previous risk assessment (Getir, 2023) carried out.

5. Conclusion

Even though the analysis of both scenarios indicates a higher risk score and a larger attack surface, it is assessed that if the mitigations suggested in the previous risk assessment are implemented, risk score can be reduced substantially. The Attack Tree Generator provides the features to analyse the impact of each mitigation implemented (i.e., by changing the risk score of a leave to see how a lower risk score can reduce the overall risk score) and helps the organisation to carry out a cost-benefit analysis.

For example, by only implementing the mitigation “M1032 – Multi-factor Authentication”, it was calculated that the overall risk score may be reduced to 3.37, a significant decrease considering the mitigation in question requires no investment and it relatively easy to implement.

The application also allows for generating partial attack trees, starting from a selected leaf node. The organisation can use this feature to focus on a specific part of a tree which may provide highest cost-benefit ratio. For instance, in the post-digitalisation scenario, “Tampering” is a branch which has a relatively high risk score with lower number of child nodes. It is possible to focus on this branch of the tree by generating a partial attack tree starting from “Tampering” leaf node:



In conclusion, given the advantages of the digitalisation and taking the attack tree of both scenarios into consideration, it is still assessed that the business should undergo a digitalisation process.

Appendices:

1. Pre-digitalisation attack tree data
2. Pre-digitalisation attack tree data short
3. Post-digitalisation attack tree data
4. Post-digitalisation attack tree data short

References:

Forum of Incident Response and Security Teams (2023) Common Vulnerability Scoring System version 3.1: Specification Document. Available from: https://www.first.org/cvss/specification-document [Accessed 13 April 2023]

Getir, E. (2023) ‘Risk Identification Report’. Paper submitted to the University of Essex Online for Information Security Management module.

Potteiger, B., Martins, G. &. Koutsoukos, X. (2016) ‘Software and Attack Centric Integrated Threat Modelling for Quantitative Risk Assessment’, *Hot Topics in the*

Science of Security (HotSos) Symposium 2016. Pittsburgh, Pennsylvania, 19-21 April. New York: Association for Computing Machinery. 99-108.

Microsoft (2022) Microsoft Threat Modelling Tool. Available from: https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-threats#stride-model [Accessed 13 April 2023].

National Institute of Standards and Technology (2012) Guide for Conducting Risk Assessments. Washington D.C.: U.S. Department of Commerce. DOI: https://doi.org/10.6028/NIST.SP.800-30r1