Risk Assessment Application Report

“Pampered Pets Executive Summary”

1. Introduction

Building upon the report submitted previously to Pampered Pets, which assesses both current and future risks associated with their business model, this executive summary offers a more concise visual representation of the potential risks facing the company. This assessment offers an **Attack Tree Generator** that is deployed in python and will allow Cathey and her associates to visually analyse the risks involved with their current data flow as well as risks associated with the proposed digitized business model.

2. Application Overview and Feature List.

The application offers the following features:

a. Accepts ***.json*** files containing threat types and data values based on the previously presented STRIDE model.
b. Evaluates the risk factor of the .json data.
c. Generates an Attack Tree with a visual representation of threats on the console.
d. Allows the user to modify risk values of dependencies or leaf nodes.
e. Exports the Attack Tree as **.png** file after risk evaluation.

Moreover, this is a **CLI-based** application and it is required to follow the steps in order to navigate the program:

1. Upload the .json file containing the data values of the threats to the program's directory. A list of files in the directory will be provided for the user to choose from. Simply copy the file name with the extension and paste it in the python console.
2. Once the file is loaded, follow the commands list to navigate through the features, it is recommended to make sure that the .json file is selected and recognized by the application. It is preferred to first test if the .json file is interpreted by plotting the tree on the console using the "plt" command. *(Check the readme file).*
3. If needed, select and modify the leaf node value by typing the name of the threat provided in the threats list. Be advised the value of the leaf nodes can only be changed. You can ask the application to calculate the result or to continue modifying other leaf values.
4. Generate the attack tree on the console, you can also allow the application to export .png version of the generated tree to the application's directory.

3. Risk Assessment Methods

The National Institute of Standards and Technology (NIST) provides several guidelines for performing quantitative threat modeling, including a likelihood of occurrence calculation (Rashid Al Asif, et al., 2022). Additionally, quantitative threat modeling involves assigning numerical values to various factors to assess the

likelihood and impact of threats. NIST recommends using available data, expert opinions, and historical incident records to estimate these probabilities as accurately as possible. The likelihood calculation is crucial in assessing the risk posed by various threats and prioritizing mitigation efforts based on their potential impact and probability of occurrence. Below is an overview of quantifying several factors to assess the likelihood calculation according to NIST's guidelines (NIST, 2012):

f. **Threat Event Frequency (TEF): Probability of the threat event.**
g. **Vulnerability Factor (VF): Probability of successful exploit.**

However, NIST suggests that the Likelihood of Occurrence (LOO) calculation can be rather discussed as a likelihood score that can be based on available experience, evidence or even expert judgment. In this case, LOO provides a simplified way to conduct risk assessment using se

semi- quantitative and qualitative values and can based on the organization's needs, context, and the nature of the threats being assessed. The formula for likelihood (L) may be represented as:

‘L = TEF x VF’

Below are the (LOO) guidelines for threat assessment as provided by the NIST:

Likelihood (LOO) - Adversarial		
Quantitative Values	**Semi-Quantitative Values**	**Description**
Very High	9.5 - 10.0	Adversary is almost certain to initiate the threat event.
High	8.0 - 9.5	Adversary is highly likely to initiate the threat event
Moderate	2.0 -7.9	Adversary is somewhat likely to initiate the treat event.
Low	0.5 - 2.0	Adversary is unlikely to initiate the threat even
Very Low	0	Adversary is highly unlikely to initiate the threat event.

Likelihood (LOO) - NON-ADVERSARIAL		
Quantitative Values	**Semi-Quantitative Values**	**Description**
Very High	9.5 - 10.0	Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year
High	8.0 - 9.5	Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
Moderate	2.0 -7.9	Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
Low	0.5 - 2.0	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

Likelihood (LOO) - THREAT EVENT RESULTING IN ADVERSE IMPACTS		
Quantitative Values	**Semi-Quantitative Values**	**Description**
Very High	9.5 - 10.0	If the threat event is initiated or occurs, it is almost certain to have adverse impacts.
High	8.0 - 9.5	If the threat event is initiated or occurs, it is highly likely to have adverse impacts.
Moderate	2.0 -7.9	If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
Low	0.5 - 2.0	If the threat event is initiated or occurs, it is unlikely to have adverse impacts.
Very Low	0	f the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.

Table 1: (LOO) values indicator

For this assessment, (LOO) values will be given to the STRIDE threat model that was previously supplemented in the risk assessment report on Pampered Pets. Both Scenarios (pre & post digitization) will be assigned (LOO) values accordingly. Refer to the tables below:

STRIDE THREAT MODEL / LOO VALUE IDENTIFIER			
Threat Type	**Description of Threat**	**Tree Node Reference**	**LOO VALUE**
Spoofing	Impersonation of users/systems	s1	2.0
	Unauthorized data access	s2	1.51
Tampering	Unauthorized data modification	t1	0.30
	Unauthorized transaction modification	t2	2.30
Repudiation	Denying actions/transactions	r1	2.60
	Falsifying evidence	r2	0.66
Information Disclosure	Unauthorized data access	i1	2.51
	Information leakage	i2	2.22
Denial of Service	System unavailability	d1	1.2
	Network resource exhaustion	d2	2.58
Elevation of Privilege	Unauthorized privilege escalation	e1	1.20
	Unauthorized access to admin functions	e2	2.58

Table 2: Pampered Pets Pre-digitization

STRIDE THREAT MODEL / LOO VALUE IDENTIFIER			
Threat Category	**Threat Description**	**Tree Node Reference**	**LOO VALUE**
Spoofing	Unauthorized access to digital systems	s1	3.1
	Impersonation of legitimate users	s2	4.55
	Falsifying digital identities	s3	6.00
Tampering	Unauthorized modification of data or software	t1	2.31
	Altering product details	t2	0.60
	Modifying order information	t3	0.60
Repudiation	Denying performed actions	r1	1.20
	False denial of orders	r2	0.66
	Denying online transactions	r3	0.66
Information Disclosure	Unauthorized access to sensitive information	i1	4.51
	Exposure of customer data	i2	5.00
	Leaking business strategies	i3	1.50
Denial of Service	Disrupting digital services	d1	0.50
	Network congestion attacks	d2	6.10
	Application-level floods	d3	6.10
Elevation of Privilege	Unauthorized escalation of user privileges	e1	3.20
	Unauthorized administrative access	e2	4.58
	User account manipulation	e3	3.00

Table 3: Pampered Pets Post-Digitization

Both tables contain a column called “**Tree Node Reference”** with a reference value for each sub threat. This allows provides a naming convention for the leaf / child nodes in an attack tree.

Attack Trees offer several benefits for visualizing, understanding, and assessing security concerns. This application will generate attack trees based on the

STRIDE model and **(LOO)** values located in the .json data. Furthermore, attack trees consist of the 3 main components:

Root node: Represents the name of the tree or that main category. In the case, the root node can be named (Pampered Pets Risk Assessment)

Node: Represents main threat category, each node can refer to a single category from the STRIDE model. (ex. Node 1 = Spoofing, Node 2 = Tampering, etc)

Leaf node/ Child node: Represents sub-category node of a parent Node, or in this case, Threats.

All nodes are referenced by *name, parent, and value* in which can be interpreted by the python application. As mentioned before, a simple naming convention will be supplemented to the **leaf nodes** according to tables 2 and 3. This provides a simpler method to visualize the tree.

The calculation of both the risk and (LOO) values is provided in the example below:

$$\textbf{Node Risk Value} = \frac{\textbf{Total Risk Value of All Leaf Nodes}}{\textbf{\textit{Total Number of Leaf Nodes}}}$$

After obtaining the value for each Node, the following calculation is commenced:

$$\textbf{Root Node Value} = \frac{\textbf{Total Risk Value of All Nodes}}{\textbf{\textit{Total Number of Nodes}}}$$

4. Results & Conclusion

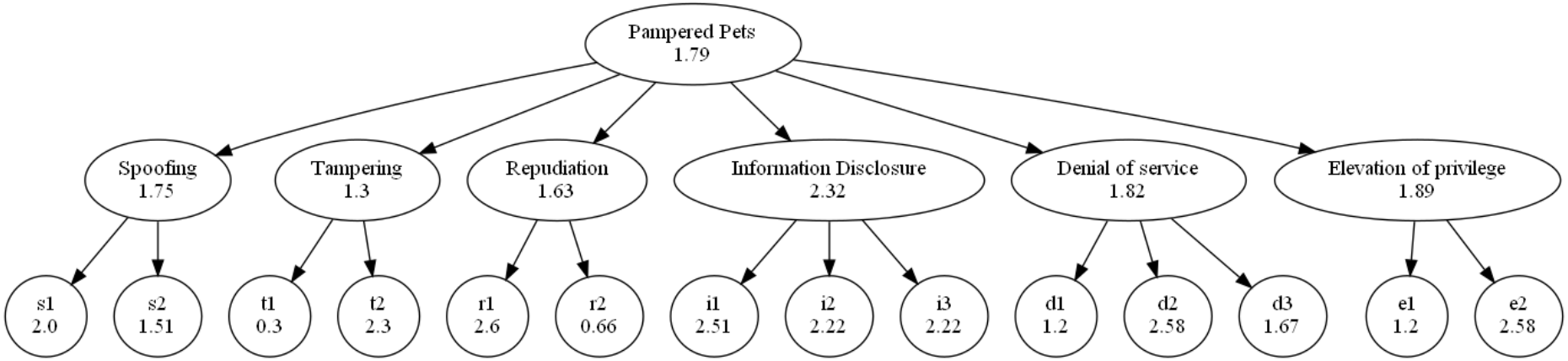

Figure 1: Attack Tree: Pampered Pets Pre Digitized

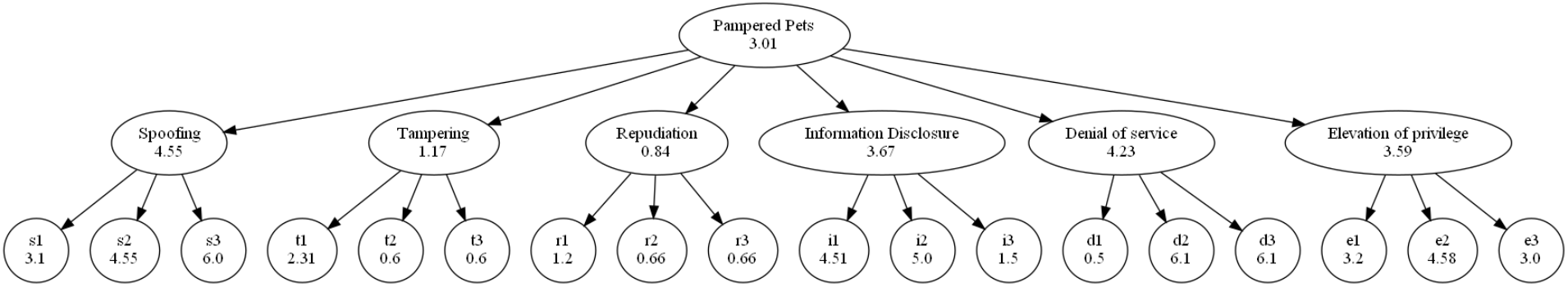

Figure 2: Attack Tree: Pampered Pets Digitized

Business Model	(LOO) (Qualitative Value)	Risk Value (Semi Quantitative Value)
Pre- Digitization	Low Risk	1.79
Post – Digitization	Moderate Risk	3.00

Table 4: Risk assessment results.

Pampered Pets digitized model exhibits a risk value escalation of **1.20 on a scale of 10** when compared to the existing business state. As outlined in the earlier section, following the LOO (Likelihood OF Occurrence) guide for risk assessment, Pampered Pets falls within the category of **Moderate Risk**. This growth in risk factor is primarily attributed to the upgraded data flow and the expansion of online assets, both of which significantly contributed to this overall assessment.

Due to a wider attack surface, the risk factor of the digitized business model witnessed an increase by **13%** of overall risk rate. While this increase may seem relatively small, mitigation strategies provided in the previous assessment can significantly contribute to the reduction of the total risk value. Additionally, the attack generator application provides the ability to modify the risk values when a mitigation use case is applied. This assists Pampered Pets to engage with an informed risk assessment tool that allows them to make a value driven decision. **In conclusion, Pampered Pets should continue to seek a digital transformation.**

References

Khan, R., McLaughlin, K. & Laverty, D., 2017. *STRIDE-based threat modeling for cyber-physical systems.* Turin, nnovative Smart Grid Technologies Conference Europe .

Rashid Al Asif, M., Hasan, K. F. & Khondoker, R., 2022. *STRIDE-based Cyber Security Threat Modeling for IoT-enabled Precision Agriculture Systems.* Dhaka, IEEE.

Mircosoft, 2009. *The STRIDE Threat Model.* [Online]
Available at: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN
[Accessed 23 08 2023].

NIST, 2012. *Guide for Conducting Risk Assessments,* Gaithersburg: National Institute of Standards and Technology.