Project Overview

The application provides functionality to import an attack tree in custom XML format, renders it graphically on a webpage, provides functionality for assigning values to the tree nodes, analyses the tree and identifies attack scenarios that are fastest or cheapest in implementation.

Applied Methodologies

Attack trees as described by Schneier (1999) are a tool for modelling security threats in a system, where the root node is the main goal of an adversary, inner nodes are subgoals where child nodes are required for a parent to succeed, and leaves are actions to achieve the goals. Values can be assigned to leaves to filter out impossible scenarios or identify those most likely to be implemented by adversaries: cheapest or fastest options.

Lopuhaä-Zwakenberg et al. (2023) offer an algorithm for aggregating values from attack tree nodes to perform a quantitative analysis of an attack tree. The algorithm suggests depth-first traversal of a tree where the values from leaf nodes are passed up the chain and then a function is applied to the available children values depending on the analysis and the node type (OR vs. AND).

The developed application will focus on the metrics such as minimum attack cost and time, and maximum damage to the enterprise. To allow for damage evaluation, loss values may be assigned to inner nodes as well, as completing a subgoal may result in damages to an enterprise on its own, for example, in case of a data breach.

Choice of Technologies

The application is implemented in the Python programming language. The business logic is organised with use of the Flask framework that integrates multiple libraries for template rendering and HTTP request processing and thus facilitates fast development of web applications (Pallets, no date).

The format of a web-based application was selected to allow both for easier data processing in Python and for implementing a graphical user interface (GUI) for visualising the tree and the reports. The tree is rendered in HTML with the use of styles developed by Ross Angus (2019).

To allow for specifying human-readable values for time periods (like `1 week`), the `humanfriendly` library is used (Odding, 2021).

Tests for the application are developed and run with the use of the `pytest` library (Krekel and pytest-dev team, no date).

Executing the Application

1. Ensure Python 3 is present. The application was developed and tested with Python 3.13.
2. In the project root, execute the command to run Flask server:

```
python -m flask run --port 8000
```

3. Open http://localhost:8000 in browser to reveal the page below:

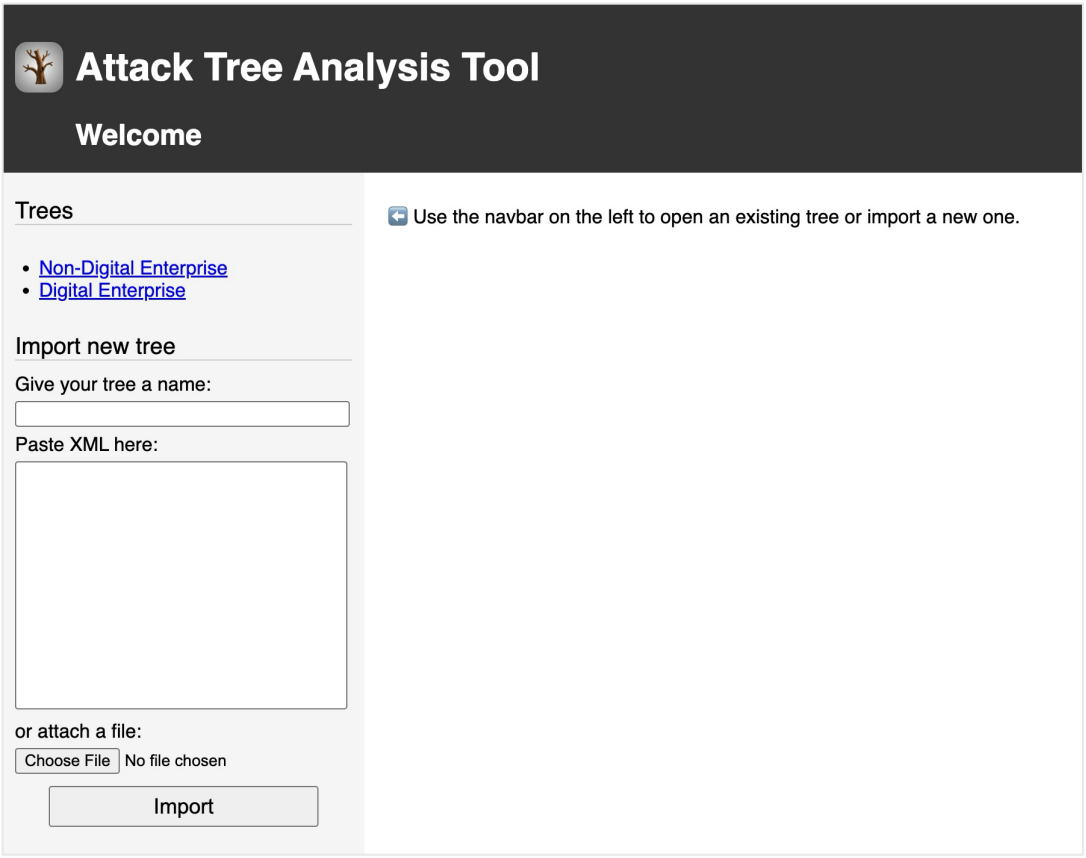


Figure 1. Application homepage

Application Design

Attack trees are represented by a tree-like data structure where each tree node is a separate object with values like attack cost, preparation time, and projected loss assigned to it. Each of the nodes includes a list of child nodes. Nodes are ‘or’ by default, i.e. child nodes are equal alternatives. A subclass is implemented to represent conjunctive ‘and’ relationship between nodes. This design, although simple, allows to describe attack trees in sufficient detail and allows to easily store and read the tree specification in the XML format.

The user-provided trees are stored in a singleton object `TreeManager` that provides a unified access point to the trees for the different application modules and functions. A

`TreeContainer` stores a tree root as well as some metadata and possible attack paths (pruned attack trees each representing a possible path from the root to an individual leaf or leaves).

Attack paths can be then wrapped in `AttackOption` class which provides methods for getting the accumulated cost, time, and loss values for the attack. An `Attack` in the application is a set of attack paths associated by a common criterion like attack cost or preparation time.

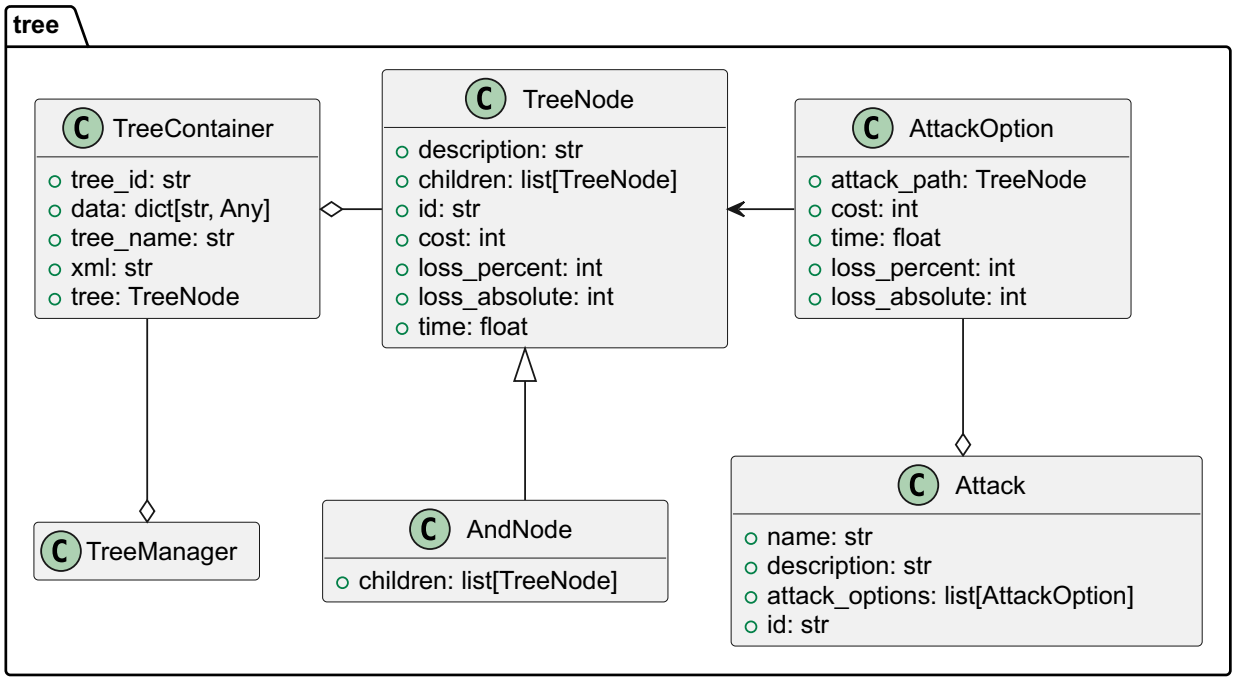


Figure 2. Class diagram for the module describing attack trees

Using the Application

1. Prepare an XML attack tree specification:

```
<node description="Attack an enterprise">
    <node description="Steal customer information">
        <node description="Access digitally stored information">
            <and>
                <node description="Access the PC physically"/>
                <node description="Unlock the PC">
                    <node description="Password is written on a note"/>
                    <node description="Guess an easy password"/>
                </node>
                <node description="Copy data to a USB drive"/>
            </and>
        </node>
    </node>
    <node description="Disrupt organisation's processes">
        <node description="Interrupt power supply"/>
    </node>
</node>
```

Figure 3. Example attack tree XML

Open the application, enter the name for the attack tree, paste the specification to the XML field, and click “Import”.

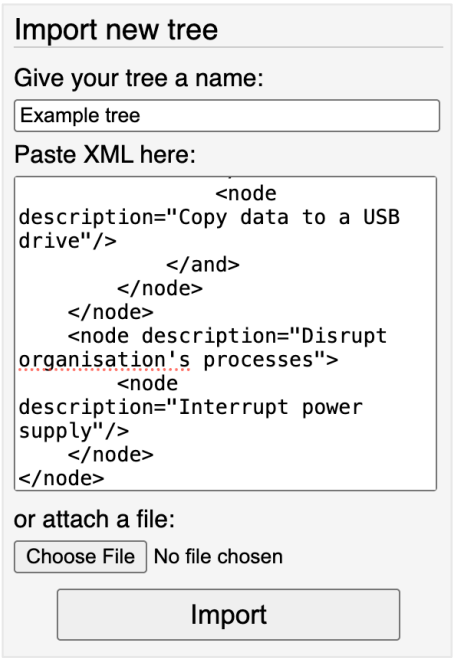


Figure 4. User interface for the import functionality

2. A page opens that renders the graphical presentation of the attack tree and allows to update values for the tree nodes. Once desired values are set, click

“Update tree” to pass the values to the backend application and recalculate the attack scenarios.

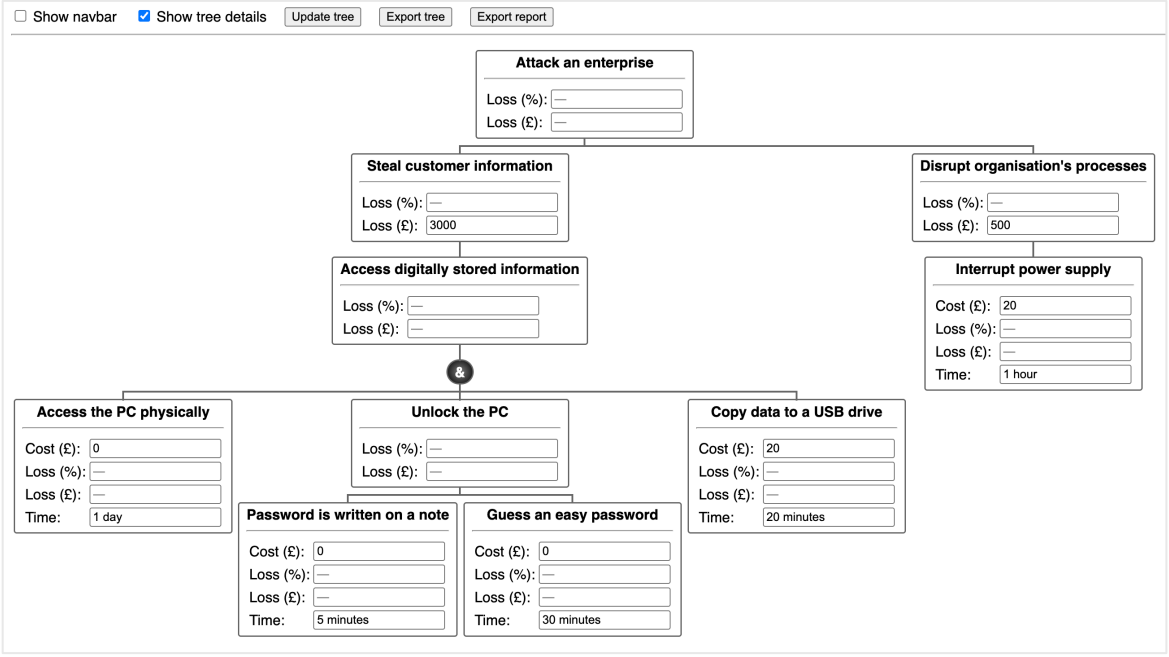


Figure 5. User interface for editing values assigned to tree nodes

3. Once values are set, scroll down to find detected attack scenarios and associated paths through the tree.

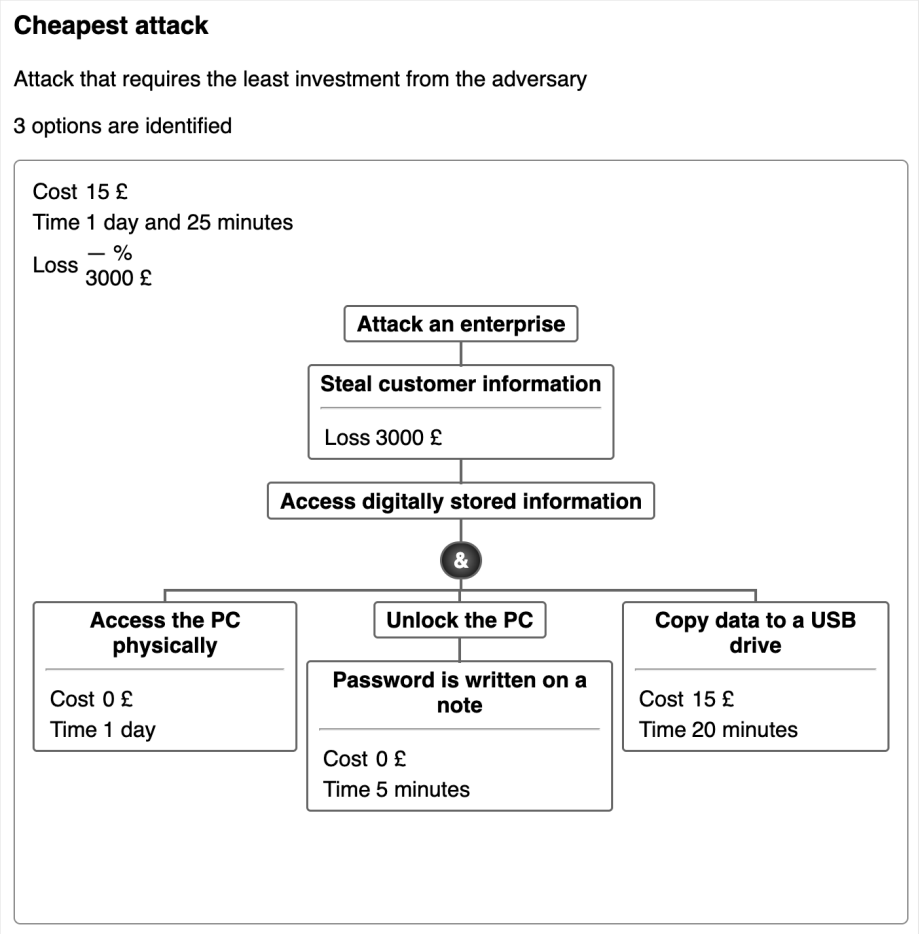


Figure 6. An example of a detected attack scenario with a rendered path

4. Export the HTML report and the XML tree specification with the new values by clicking “Export report” and “Export tree”.

Attack Tree Analysis for Pampered Pets

Based on the analyses prepared earlier, attack trees were designed for both current state of the enterprise and its digitalised version. The attack trees are included with the application sources and are loaded automatically during the application setup. Both threes are accessible via the application’s navigation menu (Figure 7).

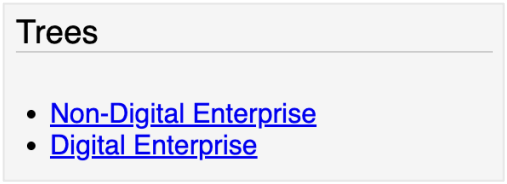


Figure 7. Navigation menu with pre-loaded attack trees for Pampered Pets

Figures and code listings in Appendices demonstrate the attack trees for both states of the enterprise.

Pre-digitalisation, the cheapest attacks don't require any investment from the adversaries yet still result in substantial damages due to reliance on human behaviour. These attacks rely on lack of access control and employees' negligence, as demonstrated on the Figure 8. Personally identifiable data disclosure leads to losses and GDPR non-compliance ("Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)," 2016; Information Commissioner's Office, 2024).

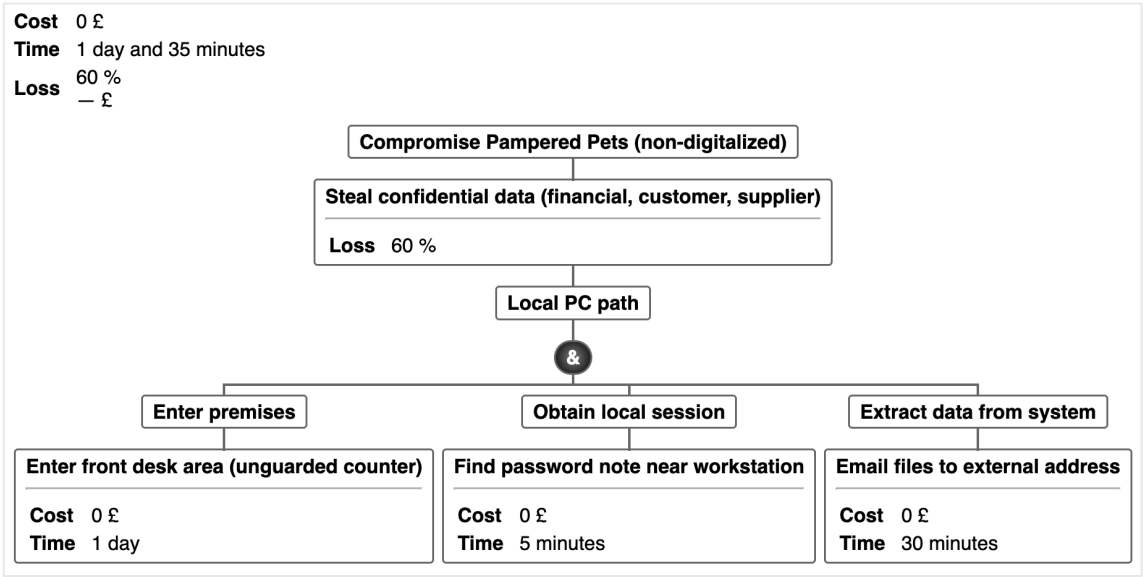


Figure 8. Scenario of an attack on non-digitalised enterprise

The fastest attacks are primarily physical, such as power supply interruption, which requires minimal preparation but only causing temporary disruption (Figure 9).

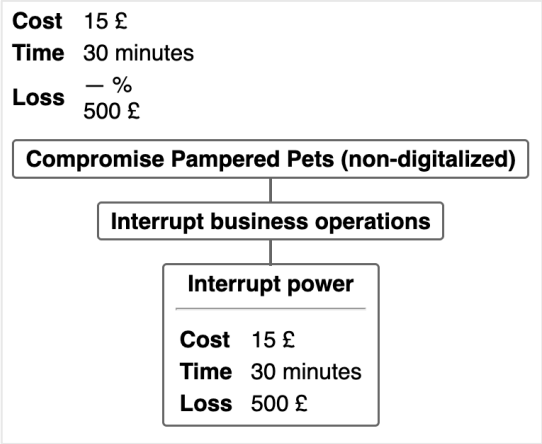


Figure 9. Fastest attack on non-digitalised enterprise

In general, physical and procedural weaknesses dominate, and human error is a recurring cause of loss.

After digitalisation, the threat landscape changes. Digital assets grow in number, and dependence on the software availability increases. The cheapest attack is now caused by software misconfiguration where critical data is available without authentication (Figure 10).

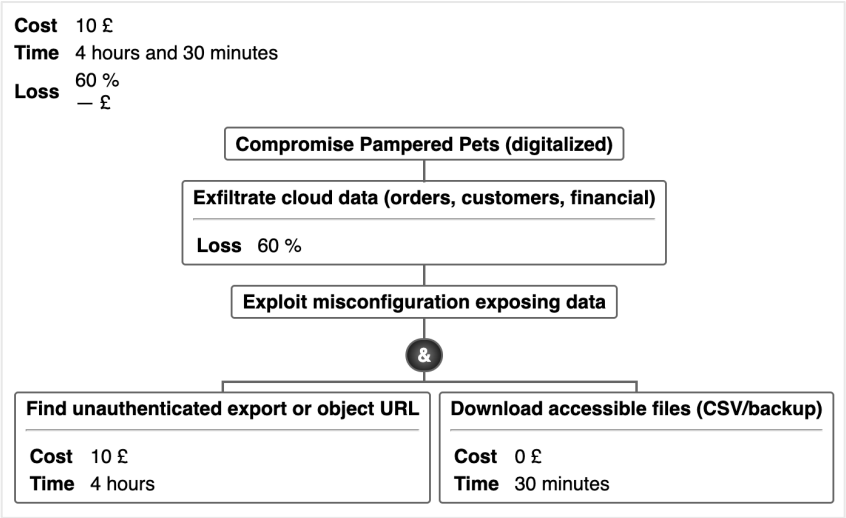


Figure 10. Cheapest attack on digitalised enterprise

Physical attacks like power interruption remain relevant, but they are still not as threatening as failures in data management, such as breaches, leaks, or backup corruption. The speed and the scale of impact are amplified in a digital enterprise. Comparatively, digitalisation introduces risks rooted in technology and data availability, as opposed to earlier human-centred weaknesses. While online presence increases revenue potential, it also requires stronger controls over data collection and processing, access management, software and hardware configuration, and backup protection.
In monetary terms, digitalisation increases potential losses, but at the same time it creates more business opportunities, and the risks can be averted by implementing appropriate security practices and due diligence.

Analysis And Conclusion

The developed application provides means to visualise attack trees and run different analyses providing a report. At the same time, it can be improved by supporting other value types for the nodes, such as probability or required skill, allowing attack trees in a form of directed acyclic graphs (Figure 11), and introducing a node type for sequential AND relationship to differentiate between events that happen in parallel vs. in sequence.

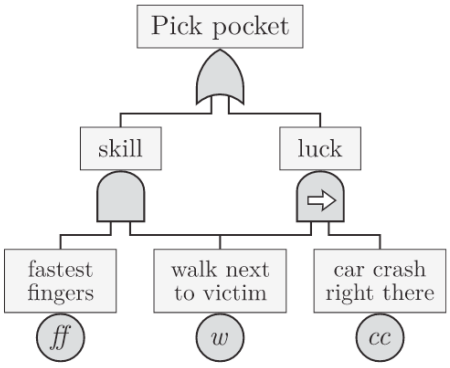


Figure 11. Attack tree in a form of a directed acyclic graph (Lopuhaä-Zwakenberg, Budde and Stoelinga, 2023)

In any case, in its current state the application already allows to contextualise attack trees for a given enterprise and provides a tool for organisation executives to better perceive the attack goals and steps and evaluate their impact on the business in interactive form. By demonstrating the change in the threat landscape after digitalisation, it can supplement the planning of the digital transformation by highlighting critical areas.

References

Angus, R. (2019) “Tree view from unordered list.” Available at: https://codepen.io/ross-angus/details/jwxMjL (Accessed: October 18, 2025).

Information Commissioner’s Office (2024) *Penalties*. ICO. Available at: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/penalties/ (Accessed: August 15, 2025).

Krekel, H. and pytest-dev team (no date) *pytest documentation*. Available at: https://docs.pytest.org/en/stable/ (Accessed: October 18, 2025).

Lopuhaä-Zwakenberg, M., Budde, C.E. and Stoelinga, M. (2023) “Efficient and Generic Algorithms for Quantitative Attack Tree Analysis,” *IEEE Transactions on Dependable and Secure Computing*, 20(5), pp. 4169–4187. Available at: https://doi.org/10.1109/TDSC.2022.3215752.

Odding, P. (2021) *humanfriendly: Human friendly input/output in Python — humanfriendly 10.0 documentation*. Available at: https://humanfriendly.readthedocs.io/en/latest/ (Accessed: October 18, 2025).

Pallets (no date) *Welcome to Flask — Flask Documentation (3.1.x)*. Available at: https://flask.palletsprojects.com/en/stable/ (Accessed: October 18, 2025).

“Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation)” (2016). Official Journal of the European Union. Available at: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: January 19, 2025).

Schneier, B. (1999) “Attack Trees,” *Schneier on Security*, December. Available at: https://www.schneier.com/academic/archives/1999/12/attack_trees.html (Accessed: October 15, 2025).

Appendix 1. Pre-Digitalisation Attack Tree XML

```
<node description="Compromise Pampered Pets (non-digitalized)">
    <node description="Steal confidential data (financial, customer, supplier)" loss-percent="60">
        <node description="Local PC path">
            <and>
                <node description="Enter premises">
                    <node description="Enter warehouse area (door left unlocked / tailgate)" cost="0" time="1 day"/>
                    <node description="Enter front desk area (unguarded counter)" cost="0" time="1 day"/>
                </node>
                <node description="Obtain local session">
                    <node description="Use unlocked session" cost="0" time="15 minutes"/>
                    <node description="Guess weak Windows password" cost="20" time="1 day"/>
                    <node description="Find password note near workstation" cost="0" time="5 minutes"/>
                </node>
                <node description="Extract data from system">
                    <node description="Open and copy spreadsheets to USB" cost="5" time="1 hour"/>
                    <node description="Email files to external address" cost="0" time="30 minutes"/>
                </node>
            </and>
        </node>
        <node description="Email account path">
            <and>
                <node description="Identify mailbox address (shop signage / receipts)" cost="0" time="1 hour"/>
                <node description="Obtain mailbox credentials">
                    <node description="Phish staff for password" cost="50" time="1 week"/>
                    <node description="Brute-force weak mailbox password" cost="20" time="1 day"/>
                </node>
                <node description="Download customer order emails (PII)" cost="0" time="30 minutes"/>
            </and>
        </node>
        <node description="Remote compromise path">
            <and>
                <node description="Deliver exploit or payload">
                    <node description="Send malicious attachment (macro/exe)" cost="50" time="1 day"/>
                    <node description="Exploit unpatched service (SMB/RDP)" cost="50" time="1 day"/>
                </node>
                <node description="Exfiltrate files over outbound channel" cost="0" time="30 minutes"/>
            </and>
        </node>
        <node description="Interception path (opportunistic)">
            <and>
```

```
                <node description="Position within Wi-Fi range" cost="20" time="1 day"/>
                <node description="Sniff plaintext email traffic (no TLS)" cost="0" time="1 hour"/>
            </and>
        </node>
        <node description="Bribe or coerce employee for access" cost="100" time="1 week"/>
    </node>
    <node description="Modify or destroy operational data" loss-absolute="1000">
        <node description="Local data tampering path">
            <and>
                <node description="Enter premises off-hours" cost="0" time="1 day"/>
                <node description="Use unlocked/shared workstation" cost="0" time="15 minutes"/>
                <node description="Delete or overwrite key spreadsheets" cost="0" time="30 minutes"/>
            </and>
        </node>
        <node description="Malware destruction path">
            <and>
                <node description="Deliver ransomware/wiper (email/USB)" cost="50" time="2 hours"/>
                <node description="Encrypt or wipe local data" cost="0" time="30 minutes"/>
            </and>
        </node>
    </node>
    <node description="Interrupt business operations">
        <node description="Exploit known crash bug to halt PC" cost="50" time="1 day" loss-absolute="500"/>
        <node description="Physically damage PCs or network hub" cost="0" time="1 day" loss-absolute="3000"/>
        <node description="Interrupt power" cost="15" time="30 minutes" loss-absolute="500"/>
    </node>
    <node description="Steal physical assets (PCs, printed records)" loss-absolute="3000">
        <and>
            <node description="Break into shop or warehouse (forced entry)" cost="0" time="1 day"/>
            <node description="Identify data-bearing items (PCs, binders)" cost="0" time="15 minutes"/>
            <node description="Remove and transport stolen items" cost="200" time="1 day"/>
        </and>
    </node>
</node>
```

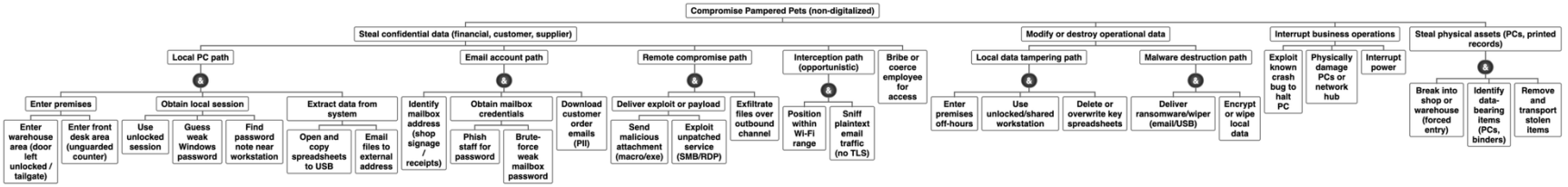
Appendix 2. Post-Digitalisation Attack Tree XML

```
<node description="Compromise Pampered Pets (digitalized)">
    <node description="Exfiltrate cloud data (orders, customers, financial)" loss-percent="60">
        <node description="Staff credential takeover to SaaS">
            <and>
                <node description="Identify login portal and target account" cost="0" time="1 hour"/>
                <node description="Obtain password">
                    <node description="Phish staff for SaaS password" cost="50" time="1 week"/>
                    <node description="Brute-force weak SaaS password" cost="20" time="1 day"/>
                </node>
                <node description="Export datasets via SaaS console/API" cost="0" time="30 minutes"/>
            </and>
        </node>
        <node description="Compromise corporate mailbox and export mail">
            <and>
                <node description="Identify mailbox address (website/receipts)" cost="0" time="1 hour"/>
                <node description="Obtain password">
                    <node description="Phish mailbox password" cost="50" time="1 week"/>
                    <node description="Brute-force weak mailbox password" cost="20" time="1 day"/>
                </node>
                <node description="Export mailbox (orders/invoices with PII)" cost="0" time="1 hour"/>
            </and>
        </node>
        <node description="Exploit misconfiguration exposing data">
            <and>
                <node description="Find unauthenticated export or object URL" cost="10" time="4 hours"/>
                <node description="Download accessible files (CSV/backup)" cost="0" time="30 minutes"/>
            </and>
        </node>
        <node description="Leverage vendor access/misconfiguration">
            <and>
                <node description="Social-engineer vendor staff to share export" cost="80" time="1 week"/>
                <node description="Download shared export" cost="0" time="30 minutes"/>
            </and>
        </node>
        <node description="Exploit SaaS defect to read records" cost="50" time="1 day"/>
    </node>
    <node description="Modify or delete cloud records (orders, stock, financial)" loss-percent="7" loss-absolute="5000">
        <node description="Change/delete via compromised staff account">
            <and>
                <node description="Obtain password">
```

```
                <node description="Phish SaaS password" cost="50" time="1 week"/>
                <node description="Brute-force weak SaaS password" cost="20" time="1 day"/>
            </node>
            <node description="Edit or delete records in console" cost="0" time="30 minutes"/>
        </and>
    </node>
    <node description="Use malware on staff PC to perform changes">
        <and>
            <node description="Deliver malicious attachment to staff PC" cost="30" time="1 day"/>
            <node description="Operate logged-in session to alter records" cost="0" time="30 minutes"/>
        </and>
    </node>
    <node description="Exploit SaaS defect causing data modification" cost="50" time="1 day"/>
</node>
<node description="Interrupt access to e-commerce/back-office/email" loss-percent="5" loss-absolute="3000">
    <node description="Launch DDoS against platform endpoints" cost="200" time="1 day"/>
    <node description="Cut local power or disconnect router" cost="15" time="30 minutes"/>
    <node description="Change shared password to lock out staff">
        <and>
            <node description="Obtain password" cost="50" time="1 week">
                <node description="Phish password" cost="50" time="1 week"/>
                <node description="Brute-force weak password" cost="20" time="1 day"/>
            </node>
            <node description="Change password and recovery options" cost="0" time="15 minutes"/>
        </and>
    </node>
</node>
<node description="Destroy/disable backups and retention" loss-percent="10" loss-absolute="2000">
    <node description="Access backup console and purge backups">
        <and>
            <node description="Obtain password" cost="50" time="1 week">
                <node description="Phish password" cost="50" time="1 week"/>
                <node description="Brute-force weak password" cost="20" time="1 day"/>
            </node>
            <node description="Delete backup sets / shorten retention to 0" cost="0" time="1 hour"/>
        </and>
    </node>
    <node description="Disable backup schedules/agents in console">
        <and>
            <node description="Obtain password" cost="50" time="1 week">
                <node description="Phish password" cost="50" time="1 week"/>
                <node description="Brute-force weak password" cost="20" time="1 day"/>
            </node>
            <node description="Disable schedules / revoke agent tokens" cost="0" time="15 minutes"/>
```

```
            </and>
        </node>
    </node>
</node>
```

Appendix 3. Pre-Digitalisation Attack Tree



Appendix 4. Post-Digitalisation Attack Tree