**Executive Summary and App Presentation**

1. **Executive Purpose & Scope**

This executive summary reports overall threat assessment ratings produced by the Python attack-tree application for Pampered Pets using the two specifications (pre\_digital.yaml and post\_digital.yaml). The scope is limited to business processes, systems, and data flows exactly as encoded in those models. The model’s top event is any modelled attack path that results in a material business loss (disruption or compromise of records or operations). Results are calculated for a 12-month horizon in GBP (£) and include:

Interpretation is constrained to the nodes, parameters, and AND/OR operators defined in the YAML files, and leaf events are treated as independent unless explicitly stated.

1. **Context and Scope**

Pampered Pets is a micro-sized UK retailer with 4 employees and predominantly face-to-face sales. This section documents how probabilities and monetary impacts were assigned to leaf nodes in the attack trees without using any sales-per-hour estimation. The figures are inputs to the Python application, which applies to the tree operators to compute annualised loss at the root. Scope is limited to processes, systems, and data flows exactly as encoded in pre\_digital.yaml and post\_digital.yaml.

1. **Methodology**

We model attack paths as an AND/OR tree. Probabilities aggregate on the structure:

* AND = product of child probabilities
* OR = . Monetary impacts are defined only on leaf events

we do not aggregate impacts at internal nodes.  
**KPIs reported:**

1. Top-event probability at the root; (ii)
2. Expected loss .

**Assumptions:** leaf probabilities are treated as conditionally independent within each gate; impacts are point estimates. Limitations (dependence, path overlap) are noted; a simple one-leaf sensitivity check is provided in the UI.

1. **Scales used for consistency**

These semi-quantitative bands anchor estimates and keeps consistency across leaves, aligned with ISO/IEC 27005’s guidance on likelihood and impact estimation (ISO/IEC, 2018).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scale | Probability (annual) | Interpretation | Impact (£) | Interpretation |
| Very Low (1) | ≤ 1% | Rare in SME context | ≤ 10,000 | Negligible operational effect |
| Low (2) | 2–10% | Possible once every few years | 10,001–50,000 | Minor financial or reputational loss |
| Medium (3) | 11–40% | Could occur annually | 50,001–100,000 | Noticeable but recoverable disruption |
| High (4) | 41–70% | Likely within the year | 100,001–250,000 | Significant disruption and costly recovery |
| Very High (5) | > 70% | Expected at least once per year | > 250,000 | Severe business or data impact |

1. **Probability assignment**

Annual probabilities were informed by empirical threat frequency and pathway data from the Verizon DBIR and ENISA Threat Landscape for small organisations and retail-relevant attack vectors (Verizon, 2024; ENISA, 2023). For power reliability, baseline outage likelihoods were aligned to UK network indicators (Ofgem, 2023). Micro-retail operational context and exposure were cross-checked against UK convenience retail characteristics to avoid overstating event rates for a four-person shop (ACS, 2024). Where only enterprise-wide rates were available, SME-appropriate subsets or conservative adjustments were applied (Verizon, 2024; ENISA, 2023).

1. **Impact estimation**

Single-loss impacts were derived from high-quality breach-cost studies and then scaled to the Pampered Pets context by selecting applicable cost components and down-weighting those unlikely to apply to a micro-retailer with limited data holdings (IBM Security, 2023; Ponemon Institute, 2023; ACS, 2024). Ransomware-related loss components (e.g., recovery labour, downtime, restoration, refunds) were anchored to ransomware cost analyses and tempered for SME scope (Ponemon Institute, 2023; IBM Security, 2023). Sector and data-depth adjustments reflect retail threat profiles summarised by ENISA (ENISA, 2023). The resulting single-loss impacts are listed per leaf below; they are inputs to the model’s aggregation and not enterprise-scale costs transplanted wholesale (IBM Security, 2023; ACS, 2024).

1. **Pre-digital attack tree: leaf estimates**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Node ID | Description | Probability | Impact (£) | ALE (£/year) |
| pos\_fail | Front-desk POS software or hardware failure | **0.50** | **£25,000** | **£12,500** |
| no\_backup | No or weak backups of sales records | **0.10** | **£180,000** | **£18,000** |
| corrupt | Spreadsheet corruption | **0.10** | **£15,000** | **£1,500** |
| delete | Accidental deletion or overwrite | **0.20** | **£25,000** | **£5,000** |
| hdd\_fail | Old warehouse PC HDD fails, no recent backup | **0.01** | **£12,000** | **£180** |
| flat\_net | Flat network, staff phones on same LAN | **0.25** | **£100,000** | **£25,000** |
| weak\_cfg | Weak Wi-Fi configuration | **0.60** | **£60,000** | **£36,000** |
| fd\_ransom | Front-desk PC ransomware encrypts records | **0.50** | **£180,000** | **£90,000** |
| power\_out | Power outage, no UPS, abrupt shutdown/data loss | **0.30** | **£8,000** | **£2,400** |
| email\_imperson | Email order impersonation and chargeback | **0.70** | **£80,000** | **£56,000** |

**Evidence notes (pre-digital):** ransomware impact and recovery components (Ponemon Institute, 2023; IBM Security, 2023); email social-engineering and fraud pathways (Verizon, 2024; ENISA, 2023); Wi-Fi and flat-network exposure patterns (ENISA, 2023); power-outage likelihood baseline (Ofgem, 2023); micro-retail operating context (ACS, 2024).

1. **Post-digital attack tree: leaf estimates**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Node ID | Description | Probability | Impact (£) | ALE (£/year) |
| sqli | SQL injection compromises data or state | **0.30** | **£90,000** | **£27,000** |
| xss | Cross-site scripting, session theft or deface | **0.30** | **£45,000** | **£13,500** |
| third\_js | Third-party JS dependency at checkout | **0.10** | **£50,000** | **£5,000** |
| weak\_controls | Weak CSP, SRI, or monitoring | **0.35** | **£70,000** | **£24,500** |
| dos\_event | Sustained traffic flood or exhaustion | **0.40** | **£40,000** | **£16,000** |
| weak\_waf\_cdn | Weak WAF, CDN, or auto-scale | **0.25** | **£100,000** | **£25,000** |
| pci | Residual PCI exposure or mis-scoped handling | **0.10** | **£100,000** | **£10,000** |
| weak\_pw | Weak password policy or credential stuffing | **0.60** | **£80,000** | **£48,000** |
| no\_mfa | No MFA on admin or staff accounts | **0.45** | **£80,000** | **£36,000** |
| public\_bucket | Publicly readable or listable object bucket | **0.20** | **£75,000** | **£15,000** |
| excessive\_perms | Over-broad IAM role enables exfiltration | **0.25** | **£60,000** | **£15,000** |
| secrets\_leak | Leaked API keys or CI secrets | **0.15** | **£60,000** | **£9,000** |
| dep\_comp | Compromised package or dependency in build | **0.15** | **£25,000** | **£3,750** |

**Evidence notes (post-digital):** web app and supply-chain attack patterns including SQLi, XSS, third-party JS, dependency risk, DDoS, and control weaknesses (ENISA, 2023); credential attacks, lack of MFA, bucket misconfiguration, excessive permissions, and secret leakage patterns (Verizon, 2024); breach-cost anchoring for data-exposure scenarios (IBM Security, 2023); retail context for exposure shaping (ACS, 2024).

1. **Assumptions and constraints**
2. **Results by scenario**

Overall threat assessment (monetary, Expected Loss, 12-month horizon, GBP):

* Pre-digital: **£121,971.80**
* Post-digital: **£88,037.50**

Supplementary probability:

* P(top) Pre: **93.96%**
* P(top) Post: **96.35%**

Comparison: **Δ = −£33,934.30** (**−27.8%**) from pre to post.

**Computation trace (from leaves to root)**

Bottom-up aggregation:

1. **Leaf level:** For each leaf with probability and single-loss impact , compute a diagnostic value: .
2. **AND node:** for children :
3. **OR node:** For children :  
   (attacker selects the cheapest successful child path)
4. **Root:** Repeat until the root is reached. Report as the overall monetary rating and as P(top).

Summing double counts parallel paths under OR nodes. The OR rules above combine probabilities while selecting one child impact to avoid double inclusion.

**Illustrative arithmetic example for an OR parent with two leaves.**  
Child A: , .  
Child B: , .  
Then  
.  
.  
.

The aggregation follows attack-tree attribute-domain semantics: AND uses product for probability and sum for cost OR uses for probability and the minimum child cost for attacker choice, as standard in the attack-tree literature (Mauw and Oostdijk, 2005; Kordy et al., 2014).

1. **Application overview**

The Python application,

* 1. **ingests** attack-tree specifications in **YAML**.
  2. **visualises** the attack tree/graph.
  3. allows the user to **edit leaf values** (probabilities and impacts) directly in the **UI**, and
  4. **aggregates** to a single overall rating at the root (monetary Expected Loss; P(top) as supplementary).

Both the **pre-digital** and **post-digital** models were run in the application to demonstrate the threat model before and after digitalisation.

**Screenshots**

**A diagram of a triangle

AI-generated content may be incorrect.**

Figure 1 - Pre-digital Attack Tree

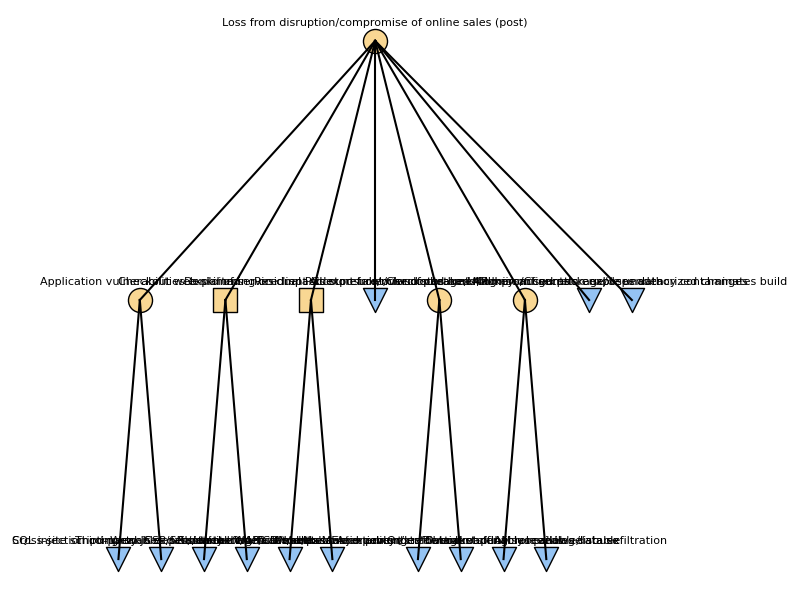
****

Figure 2 - Post-digital Attack Tree

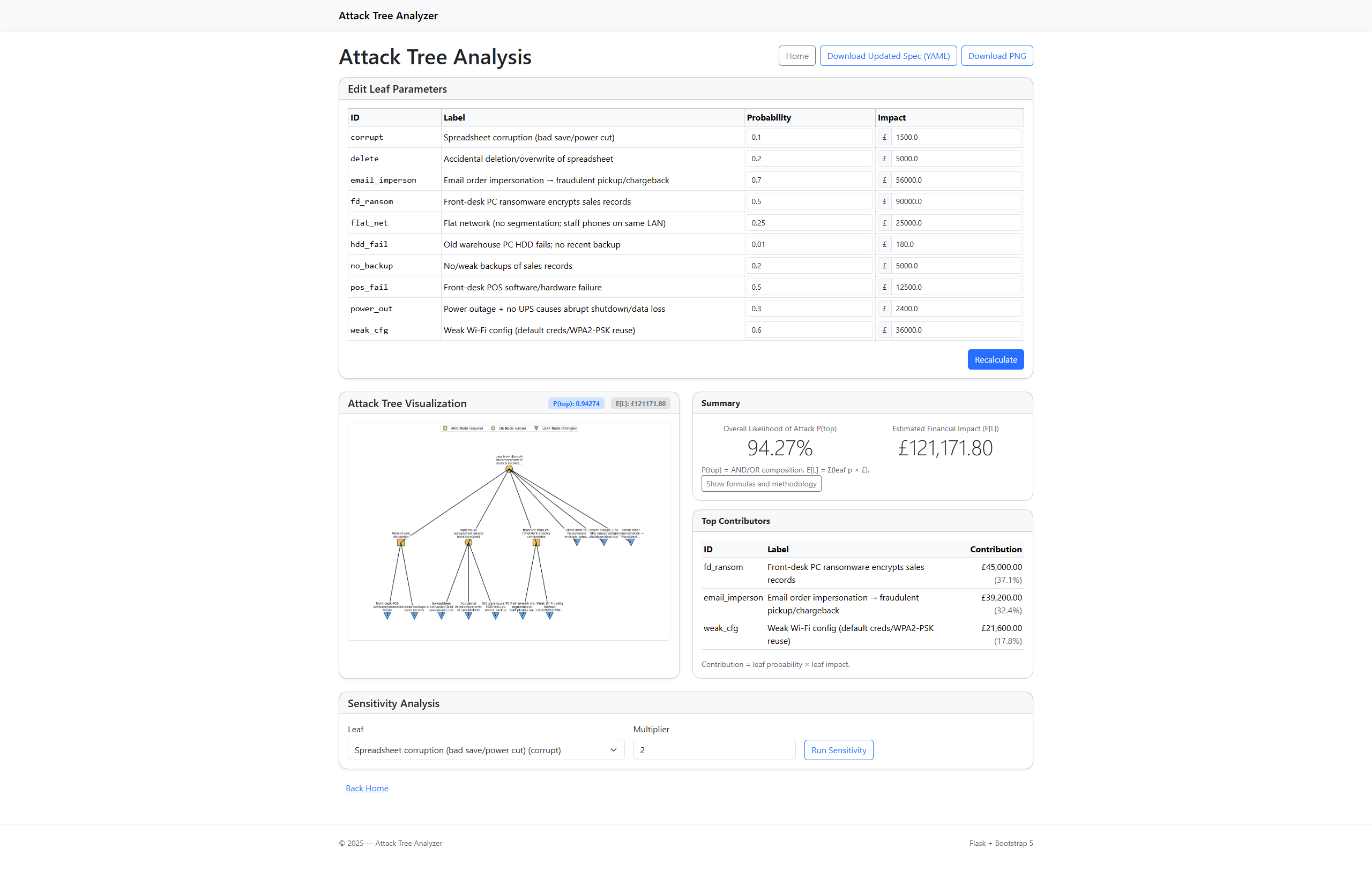


Figure 3 - Attack Tree Analyzer Screenshot for Pre-digital

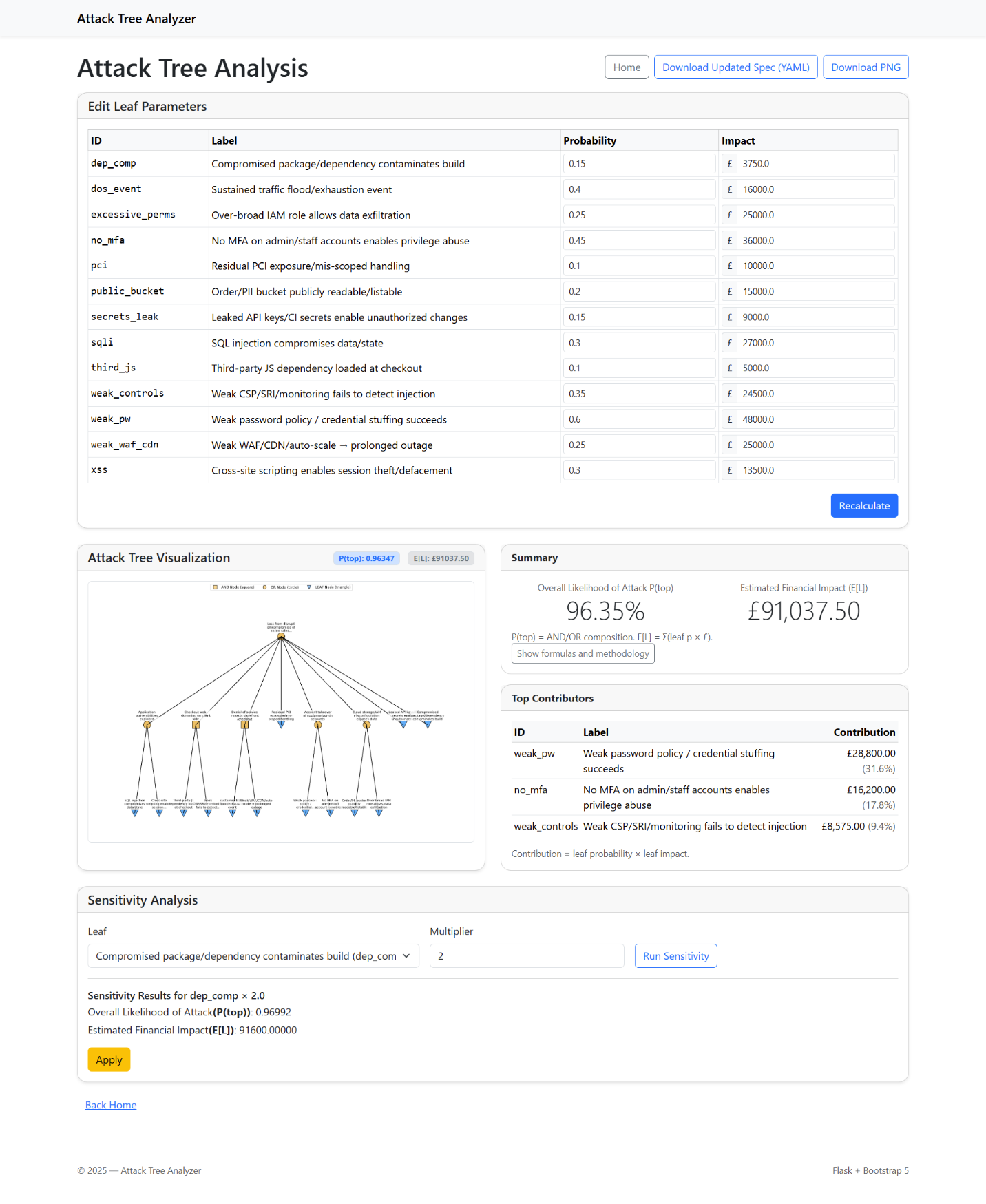


Figure 4 - Attack Tree Analyzer Screenshot for Post-digital

**References**

Association of Convenience Stores (ACS) (2024) Local Shop Report 2024. ACS. Available at: <https://cdn.acs.org.uk/public/ACS%20Local%20Shop%20Report%202024%20%28low%20res%29.pdf> (Accessed: 19 October 2025).

ENISA (European Union Agency for Cybersecurity) (2023) ENISA Threat Landscape 2023. Heraklion: ENISA. Available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023> (Accessed: 19 October 2025).

IBM Security (2023) Cost of a Data Breach Report 2023. IBM Corporation. Available at: <https://d110erj175o600.cloudfront.net/wp-content/uploads/2023/07/25111651/Cost-of-a-Data-Breach-Report-2023.pdf> (Accessed: 19 October 2025).

ISO/IEC (2018) ISO/IEC 27005:2018 Information security risk management. Geneva: International Organization for Standardization and International Electrotechnical Commission. Available at: <https://www.iso.org/standard/75281.html> (Accessed: 19 October 2025).

Kordy, B., Mauw, S., Radomirović, S. and Schweitzer, P. (2014) ‘Attack–defence trees’, Journal of Logic and Computation, 24(1), pp. 55–87. <https://doi.org/10.1093/logcom/exs029>

Mauw, S. and Oostdijk, M. (2005) ‘Foundations of attack trees’. In: Won, D. and Kim, S. (eds.) Information Security and Cryptology: ICISC 2005. Lecture Notes in Computer Science, 3935. Berlin and Heidelberg: Springer, pp. 186–198. Available at: <https://link.springer.com/chapter/10.1007/11734727_17> (Accessed: 19 October 2025).

Ofgem (2023) Energy network indicators (data portal). Office of Gas and Electricity Markets. Available at: <https://www.ofgem.gov.uk/news-and-insight/data/data-portal/energy-network-indicators> (Accessed: 19 October 2025).

Ponemon Institute (2023) The Global Cost of Ransomware Study. Ponemon Institute. Available at: <https://www.illumio.com/resource-center/cost-of-ransomware> (Accessed: 19 October 2025).

Verizon (2024) Data Breach Investigations Report (DBIR). Verizon Business. Available at: <https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf> (Accessed: 19 October 2025).