Outlier Handling Techniques Report

Below are the top five methods for detecting and treating outliers in your cyber-attack classification dataset. Copy and paste into Obsidian as-is.

Top 5 Outlier-Handling Techniques

1. Winsorization (Percentile-Based Capping)

Description:
Replace values below the p-th percentile and above the $(100 - p)$-th percentile with the corresponding percentile values.

Why Try:
Limits extreme distortions without dropping any records.

How It Helps:
Prevents rare, extreme flows from dominating tree splits or creating overly deep branches.

---

2. Direct Removal

Description:
Identify outliers (e.g. via IQR or Z-score rules) and drop those records entirely from the dataset.

Why Try:
Straightforward and effective when outliers are clearly erroneous or noise-driven.

How It Helps:
Ensures invalid or corrupted flow records (e.g. negative durations, infinities) do not skew model training.

---

3. Z-Score Trimming

Description:
Compute Z-scores $Z = \frac{x-\mu}{\sigma}$ and flag $|Z| > k$ (e.g. $k = 3$) as outliers; then drop or cap them at

$\pm k\sigma$.

Why Try:
Provides a statistically principled rule for approximately Gaussian features.

How It Helps:
Systematically controls variance and removes or limits extreme packet-rate or duration values.

---

4. Log1p + Winsorization Combo

Description:

1. Apply a log1p transform $\log(x+1)$ to compress right-skewed features.
2. Winsorize at chosen percentiles (e.g. 1st/99th).

Why Try:
Addresses long tails and any remaining extremes in one simple pipeline.

How It Helps:
Reduces skew, improves histogram quality for HGB and gain calculations for boosters, and caps residual outliers.

---

5. Isolation Forest

Description:
An unsupervised model that builds random “isolation trees”; points requiring fewer splits to isolate receive higher anomaly scores.

Why Try:
Captures complex, multivariate outliers that simple thresholds miss.

How It Helps:
Flags atypical combinations of flags, rates, and durations—remove or down-weight these before training.
