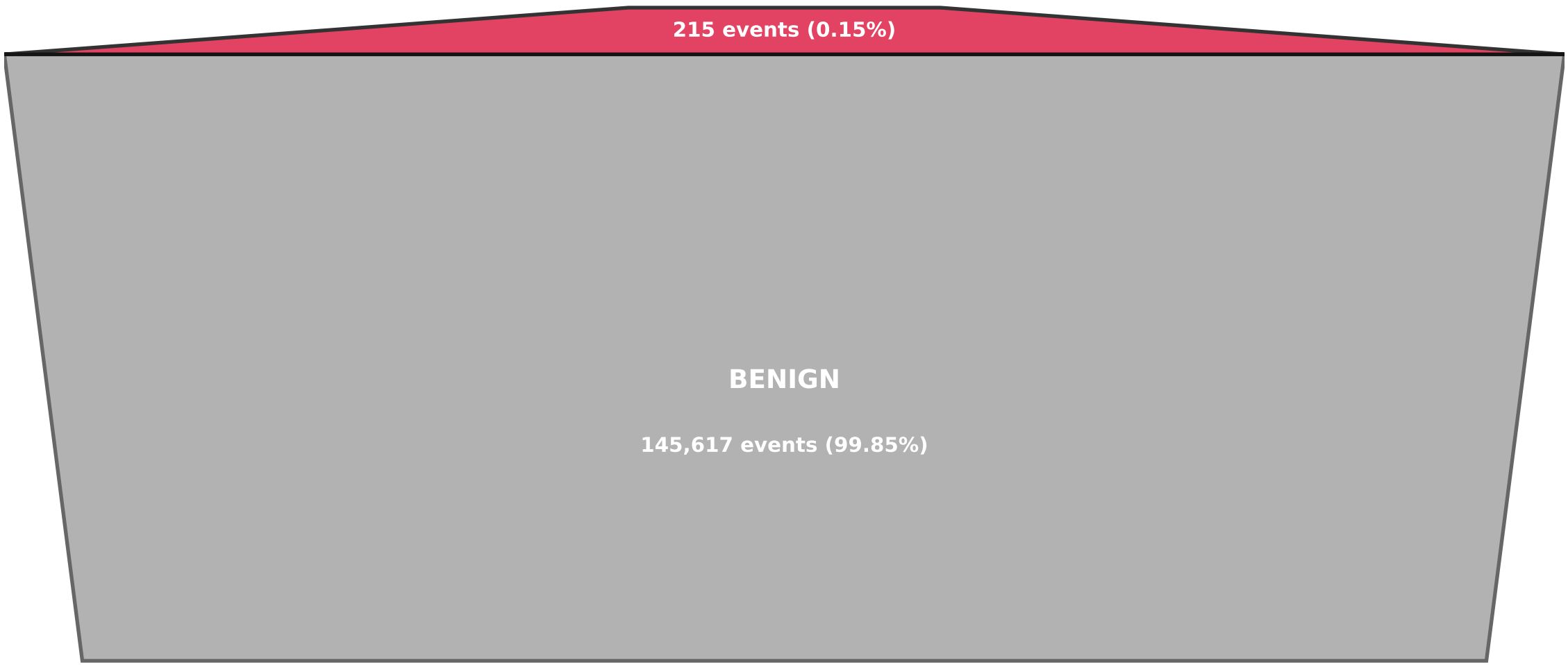
Figure 8.2: Labeled Sysmon Dataset Distribution

Binary Classification: Benign vs. Malicious Events



Imbalanced Dataset Challenge

Requires: SMOTE, Class Weighting, or Anomaly Detection Methods