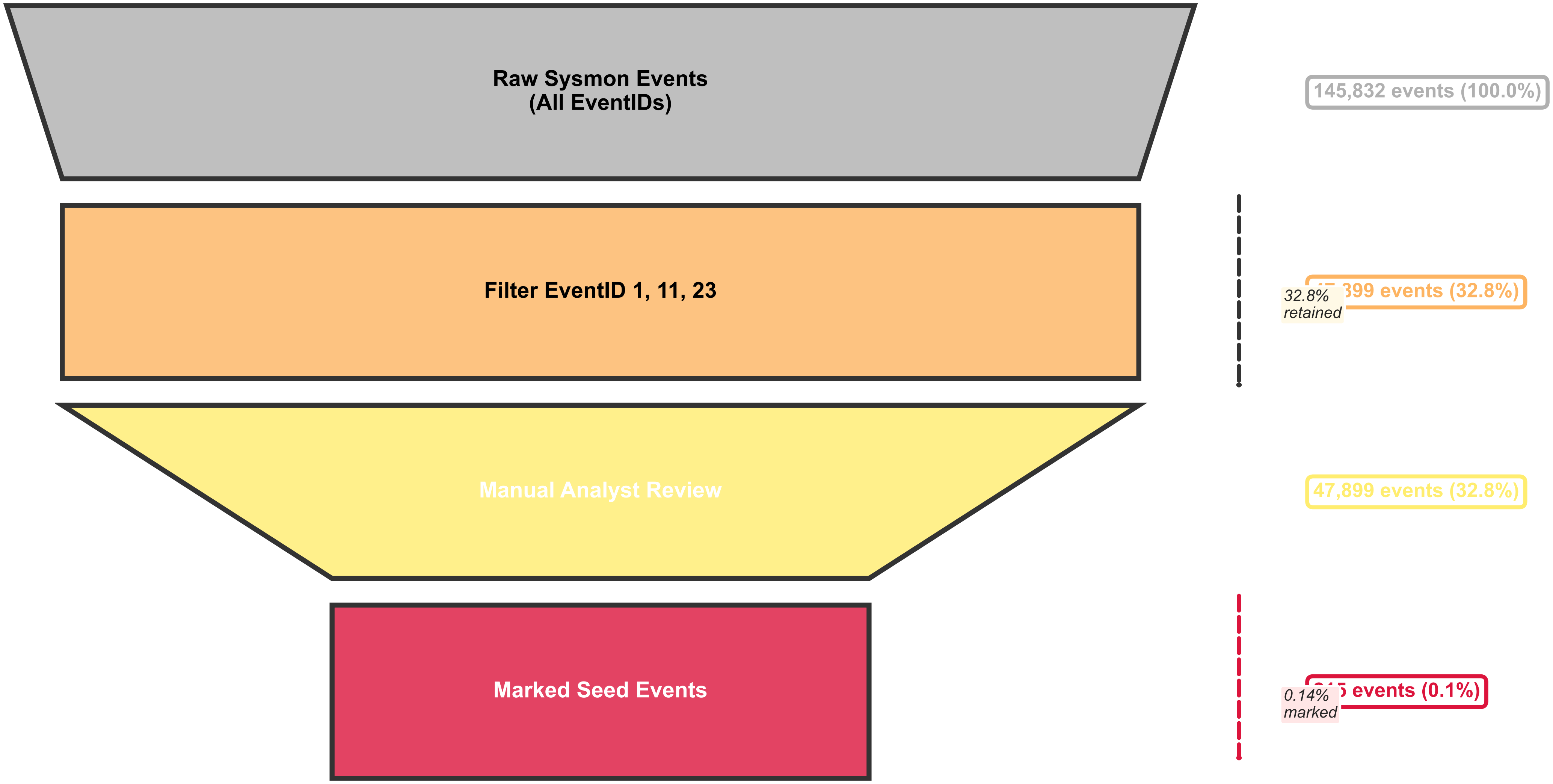
Figure 6.1: Target Event Filtering Logic

Sysmon Seed Event Extraction Funnel



Human analyst reviews extracted events and marks significant attack operations as "seed events" with MITRE ATT&CK Tactic and Technique labels for downstream lifecycle tracing.