POSTER PITCH

1. Opening
"Imagine you're monitoring millions of financial transactions per second, or defending a cloud service against the next zero-day attack. You can't afford to miss a single anomaly—or to be flooded by false alarms."

2. Highlight Problem Statement
"In streaming contexts—cloud logs, market feeds, cybersecurity—data distributions shift over time (concept drift), labels are scarce, and heuristic detectors give no statistical guarantees. How do you dynamically detect rare, extreme events without assuming a fixed data distribution or manually tuning thresholds?"

3. Key Idea & Background
"Our work brings **Extreme Value Theory (EVT)**—the statistical backbone behind flood-levee design—into streaming anomaly detection. EVT's Peaks-Over-Threshold (POT) theorem tells us that values exceeding a high threshold converge to a Generalized Pareto Distribution (GPD). By fitting a GPD online, we can set quantile-based decision thresholds that guarantee any desired false-positive rate."

4. Algorithms (Siffer et all, 2017)
- **SPOT** (Streaming POT) applies POT directly on the incoming stream:
  - **Initialization:** fit a GPD on the first ~1 000 points to get a starting threshold.
  - **Online:** every time a new point exceeds that threshold, treat it as a peak, update the GPD fit, and recompute the threshold—so the bound adapts continuously.
- **DSPOT** handles **concept drift** by first detrending each observation (subtracting a moving average) and then running SPOT on the residuals. This lets us track non-stationary baselines—e.g. daily seasonality or slow shifts—while still detecting the true extremes.

5. Results Highlights
- On **network traffic** (MAWI): SPOT achieved 86 % true-positive rate with under 4 % false-positives in detecting SYN-flood scans.
- On **NAB benchmark** (occupancy sensor): DSPOT pinpointed real anomalies with only one false alarm.
-

6. Contributions & Future Paths
- **First** large-scale EVT evaluation on streaming benchmarks.
- **Comparative** against ADWIN + Isolation Forest, RRCF, HTM
- **Extensions** in progress: adaptive window sizing for faster re-calibration, hybrid switching between SPOT/DSPOT via explicit drift

detectors, and applying POT on anomaly **scores** rather than raw values.

7. Bye bye
“With SPOT and DSPOT, you get principled, online, self-tuning anomaly detectors—with **false-positive rates you choose**, and **no assumptions** on your data’s distribution—ready for any real-world streaming application.”