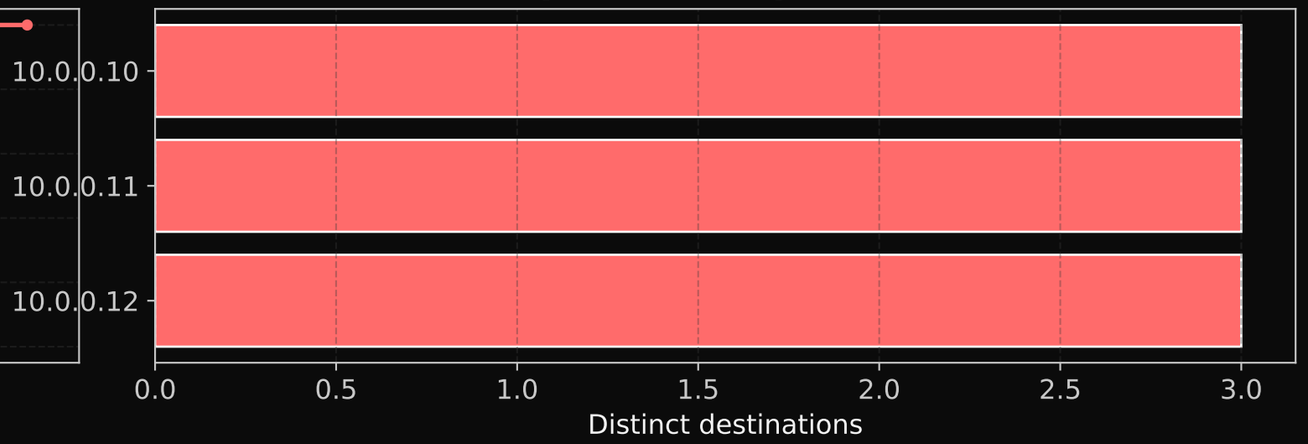
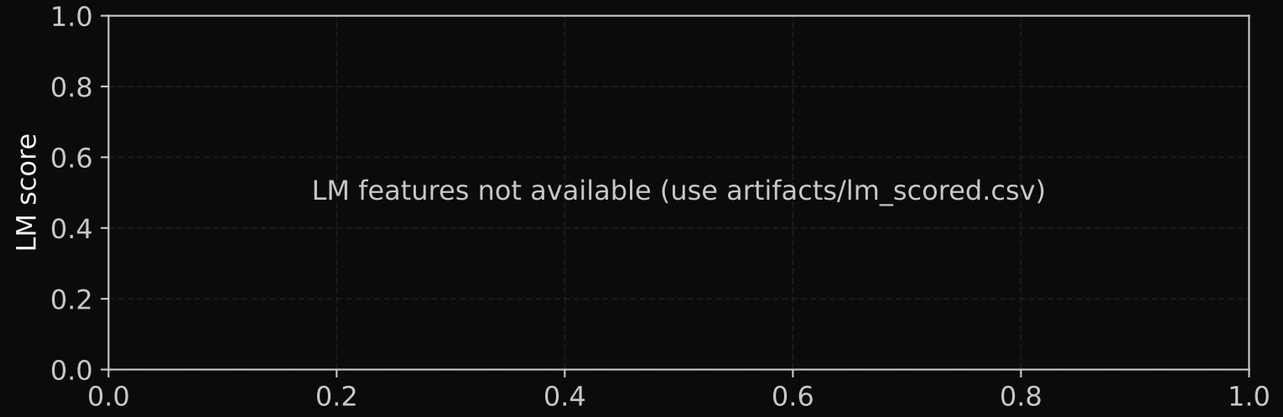
Alert rate over time (1-min buckets)

Top sources by fan-out



Lateral-Movement score over time




```
Top high-risk events (max 8):
2025-06-12 12:00:00 | 10.0.0.11   → 10.0.0.6   :22    | sev=1  | lm=0.0
2025-06-12 12:00:20 | 10.0.0.11   → 10.0.0.6   :22    | sev=0  | lm=0.0
2025-06-12 12:01:00 | 10.0.0.11   → 10.0.0.7   :22    | sev=4  | lm=0.0
2025-06-12 12:01:20 | 10.0.0.11   → 10.0.0.7   :22    | sev=0  | lm=0.0
2025-06-12 12:02:00 | 10.0.0.10   → 10.0.0.7   :80    | sev=2  | lm=0.0
2025-06-12 12:02:20 | 10.0.0.10   → 10.0.0.7   :80    | sev=0  | lm=0.0
2025-06-12 12:03:00 | 10.0.0.12   → 10.0.0.6   :443   | sev=3  | lm=0.0
2025-06-12 12:03:20 | 10.0.0.12   → 10.0.0.6   :443   | sev=0  | lm=0.0
```

- Investigate sources with unusually high fan-out (many distinct internal destinations).
- Prioritize correlated alerts (Suri+Zeek) — they carry stronger confidence.
- Watch for rising LM-score clusters in short windows (possible lateral burst).
- Exports: artifacts/dashboard_page1.png/.pdf and artifacts/dashboard_page2.png/.pdf