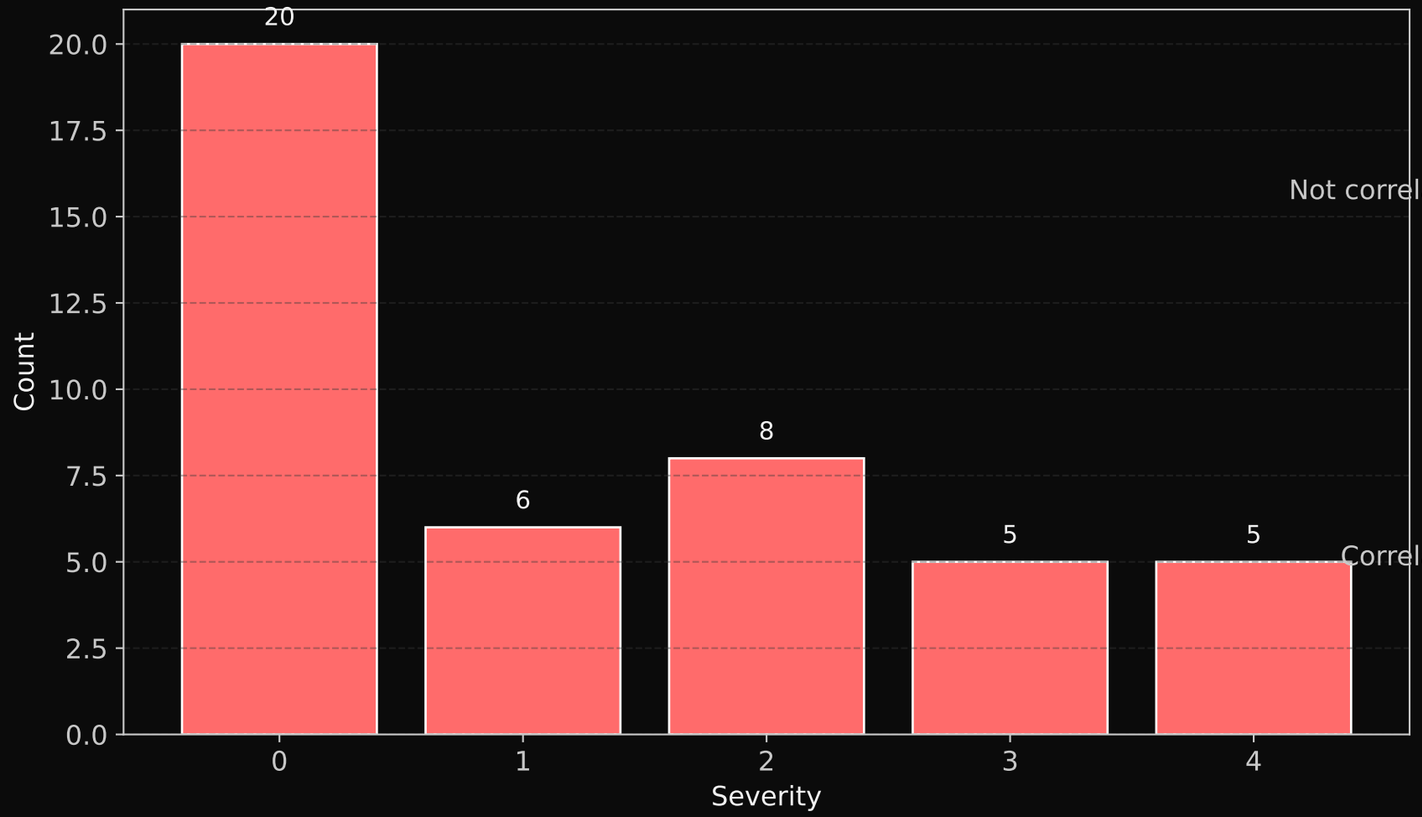
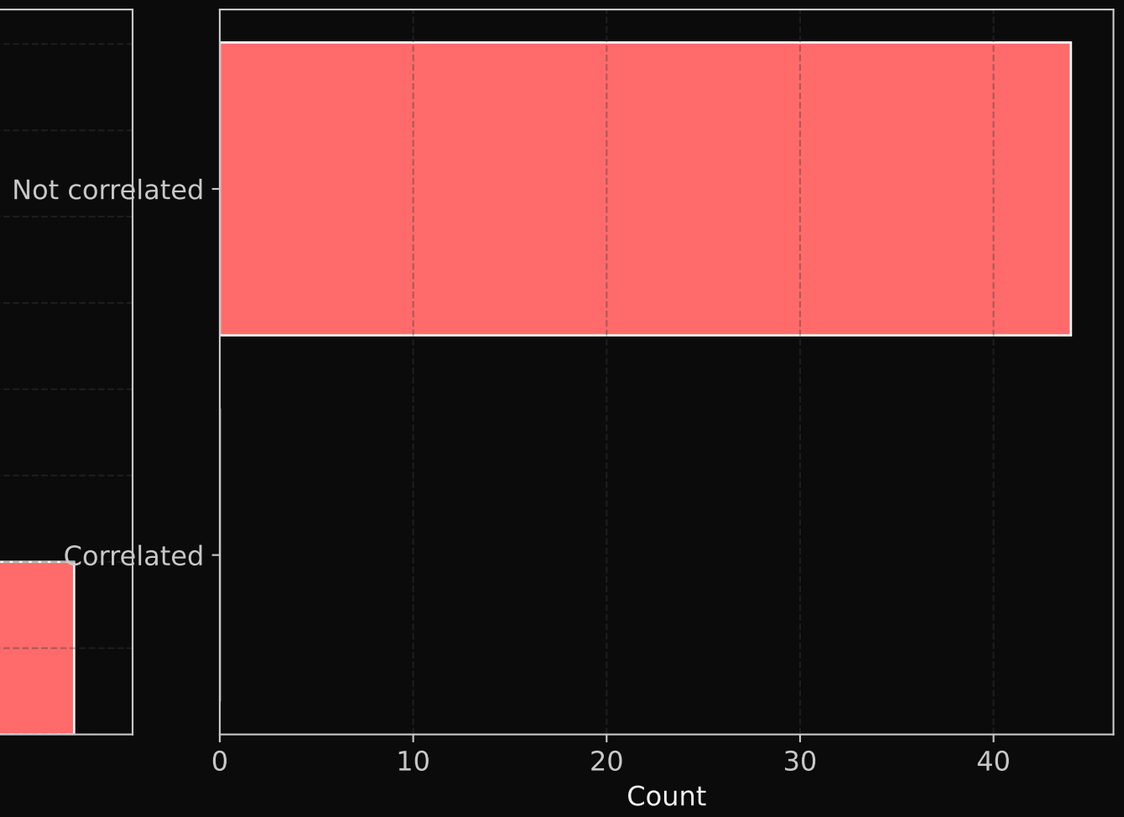
NetSentinel — Basic Alert Overview

Total alerts	Correlated (Suri+Zeek)	High risk (LM≥60)	Unique src hosts	Unique dest hosts	Max fan-out (src→dests)
44	0	0	3	3	3

Alert Severity Distribution



Suri↔Zeek Correlation



- Purpose: fuse Suricata alerts with Zeek flows to surface early indicators of lateral movement.
- “Correlated” = a Zeek flow confirms context for a Suricata alert (same 5-tuple within 60 seconds).
- LM score combines severity, correlation, fan-out, and risky ports (e.g., 445/3389).
- Dataset span (UTC): 2025-06-12 12:00:00+00:00 → 2025-06-12 12:23:20+00:00