■ Log Correlation Breakdown Diagram

```
■ Log Correlation Diagram (ASCII)

   Normal Time Flow:

   client1 --> [23:00] LOGIN         logserver --> [23:00] LOGIN
   client2 --> [23:01] CMD_EXEC      logserver --> [23:01] CMD_EXEC

   Time Drift Scenario:

   client1 --> [23:00] LOGIN         logserver --> [23:00] LOGIN
   client2 --> [23:06] CMD_EXEC      logserver --> [23:06] CMD_EXEC

   ■ Result: Impossible timeline for correlation
   ■ Impact: SIEM alerts fail, IR confusion, incident response delay

   ■ Challenge:
   - Write a parser that flags logs out of sync
   - Normalize timestamps or group by host
```