Splunk to Sentinel Logic

bin time doc

> | summarize initial_time = min(TimeGenerated), end_time = max(datetime_add("Second",1,TimeGenerated)) by bin(TimeGenerated,15m), src_user

---

Revision #1
Created 2022-04-12 13:58:02 UTC by Clinton
Updated 2022-04-12 13:59:51 UTC by Clinton