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 12 April 2022 13:58:02 by Clinton
Updated 12 April 2022 13:59:51 by Clinton