

Splunk Use Case tracker

```
| rest splunk_server=local count=0 /services/saved/searches
| where disabled=0
| rename action.correlationsearch.label as csearch_label, alert.suppress.period as Throttling,
alert.suppress.fields as "Grouped By", action.notable.param.rule_title as "Notable Title",
action.notable.param.drilldown_search as "Drilldown Search", updated as "Last Updated",
actions.email.to as "Email Recipients"
| search "Notable Title"="*TUC*"
| convert num(Throttling)
| eval "Throttling (Days)"=Throttling/86400
| table csearch_label, "Notable Title", description, search, "Drilldown Search", "Throttling
(Days)", "Grouped By", cron_schedule, dispatch.earliest_time, dispatch.latest_time, author,
actions, "Email Recipients", "Last Updated"
```

Revision #2

Created 23 March 2022 14:59:18 by Clinton

Updated 23 March 2022 15:06:01 by Clinton