Splunk

- Splunk Use Case tracker
- Splunk total run time
- Splunk Drill Down Events
- Splunk Results Token

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"
```

Splunk total run time

```
(index=_audit host=* action=search sourcetype=audittrail search_id!="rsa_*")
| eval user = if(user="n/a", null(), user)
| eval search_id=replace(search_id, "'(.*)'", "\1")
| eval search=if(isnull(savedsearch_name) OR savedsearch_name=="", search, savedsearch_name)
| stats min(_time) as _time, values(user) as user, max(total_run_time) as total_run_time,
first(search) as search, first(apiStartTime) as apiStartTime, first(apiEndTime) as apiEndTime
by search_id
```

Splunk Drill Down Events

```
earliest=$initial_time$ latest=$end_time$ index=$index$ EventCode=4624 NOT Logon_Type IN ("5")
host=$orig_host$
```

> orig_action_name
> orig_host
> orig_rid
> orig_sid

Splunk Results Token

fieldsummary