Rule Sample

Log Analytics:

> Logs

Rules

> Analytics

```
OfficeActivity
| where ingestion_time() > ago(5m)
| where tolower(OfficeWorkload) matches regex "onedrive|sharepoint" and tolower(Operation)
matches regex "filesyncdownload|filedownload" and UserId != "app@sharepoint"
| summarize initial_time = min(TimeGenerated), end_time =
max(datetime_add("Second",1,TimeGenerated)), operation=make_set(Operation,5),
workload=make_set(OfficeWorkload,5), file_name=make_set(SourceFileName,5),
file_count=dcount(OfficeId) by bin(TimeGenerated,5m),UserId, ClientIP
| project-rename src_ip=ClientIP, src_user=UserId
| where file_count>500
```

Revision #1
Created 2022-03-21 17:50:04 UTC by Clinton
Updated 2022-03-21 17:51:46 UTC by Clinton