



dataaaa

```
index=wineventlog  
sourcetype=WinEventLog:Security  
(EventCode=4728 OR EventCode=4732)
```

```
| eval Group_Name=if(EventCode==4728, "Admins",  
"RDP Users")
```

```
| table _time, EventCode, Group_Name,  
Account_Name
```

```
| sort - _time
```

[Read More](#)