**SEIM solutions**

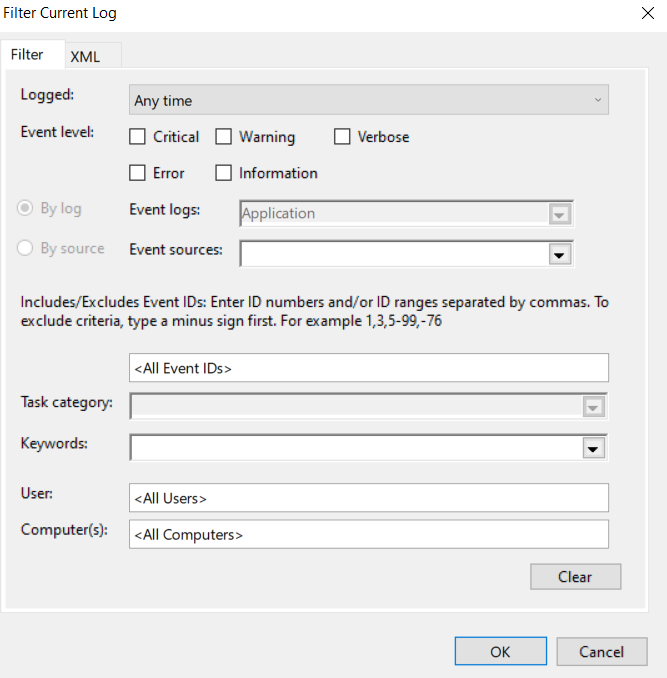
**Security information and event management using Splunk**

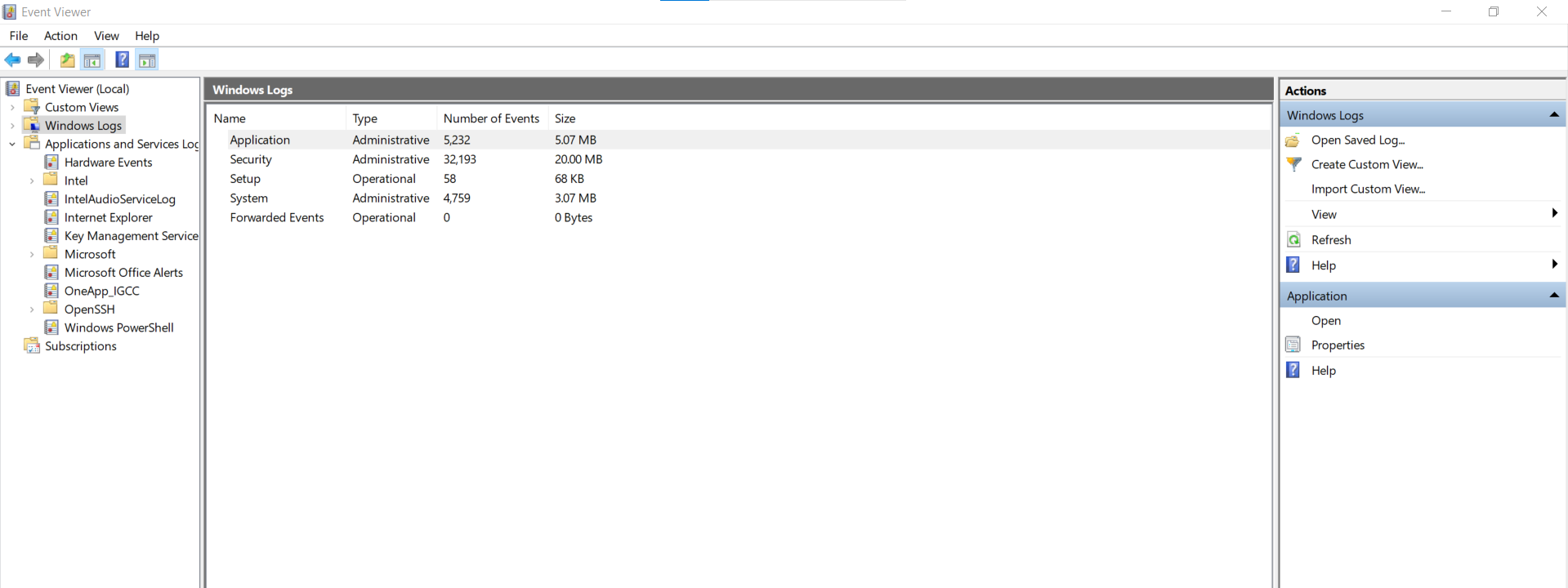
Event viewer works as splunk it has all the system logs everything that happens on your device

Application , security , system , setup logs all of it

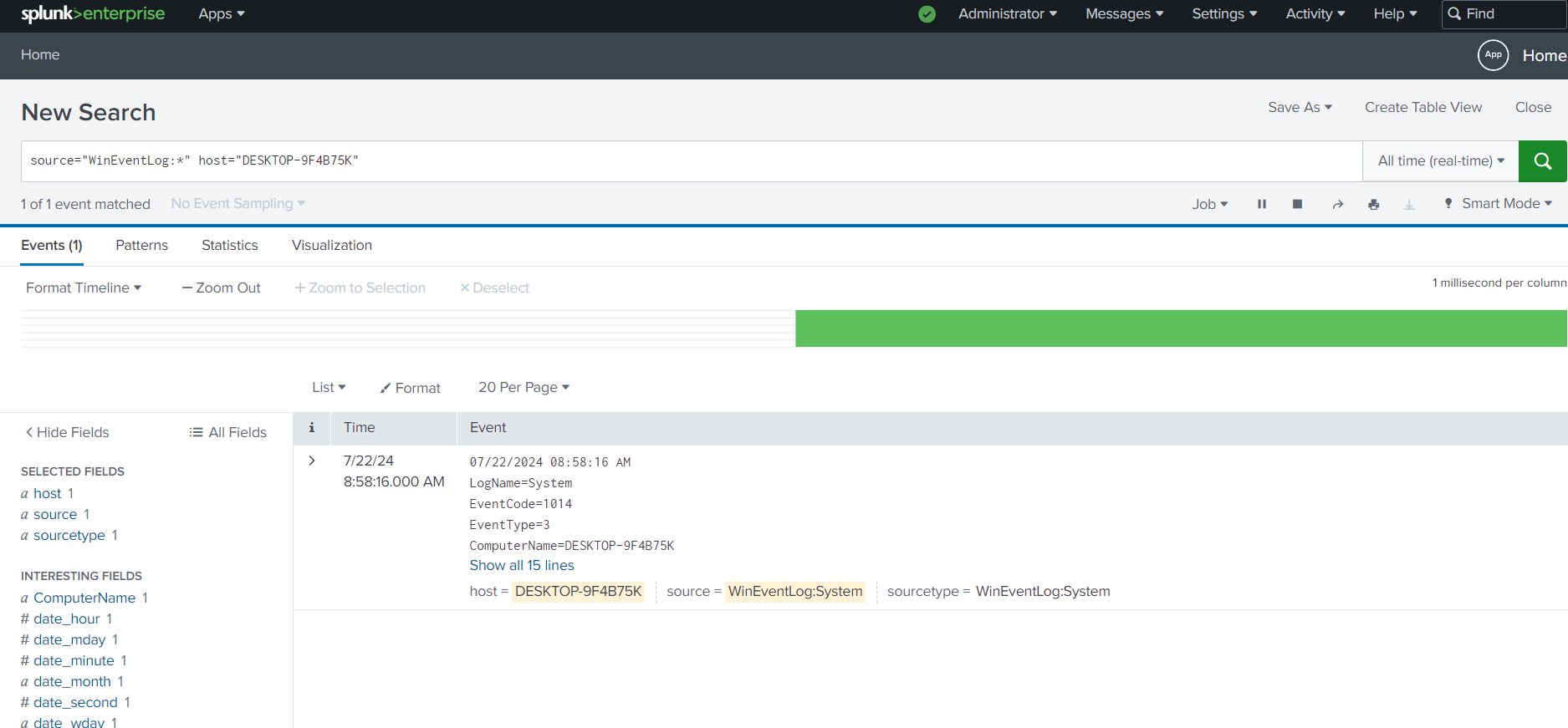
We have to check this always to see if something happened or someone tried to log into my device

We can filter the logs critical , warning , error

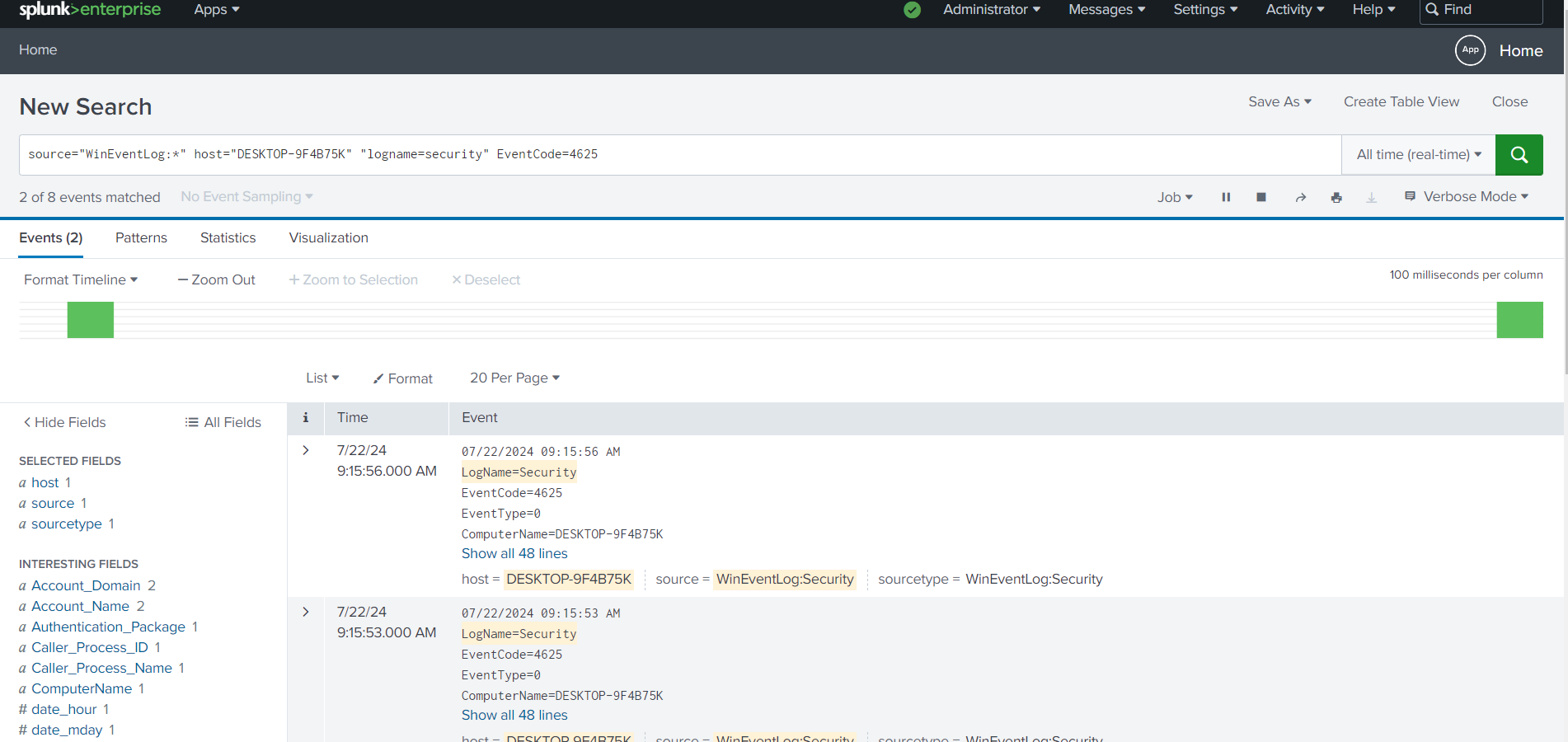
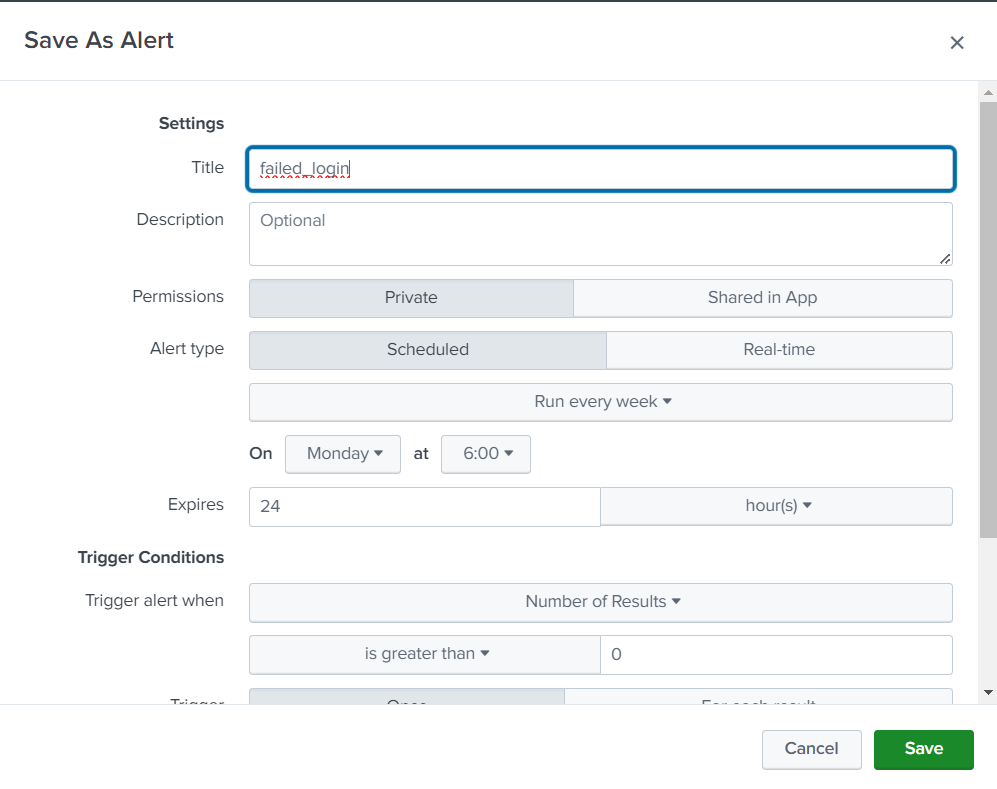




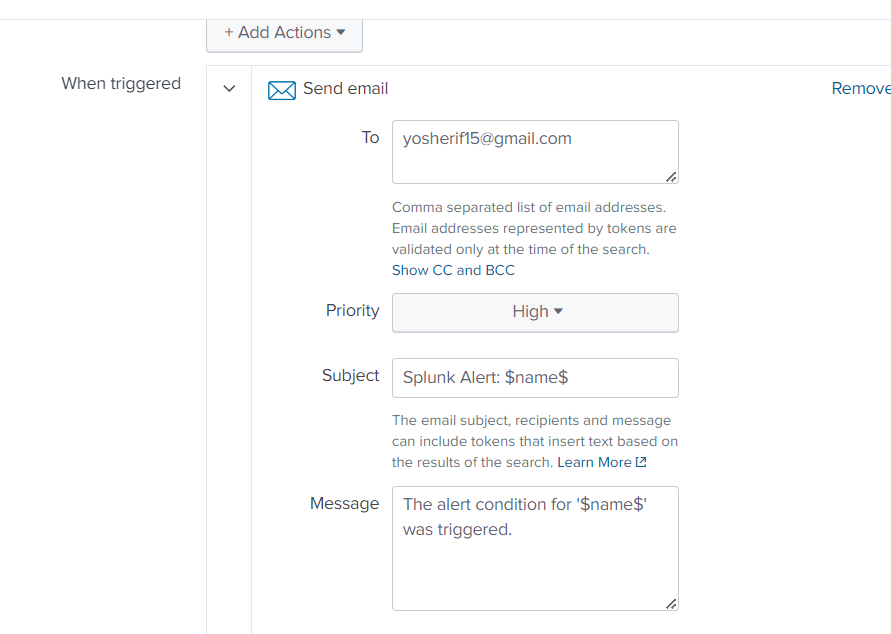
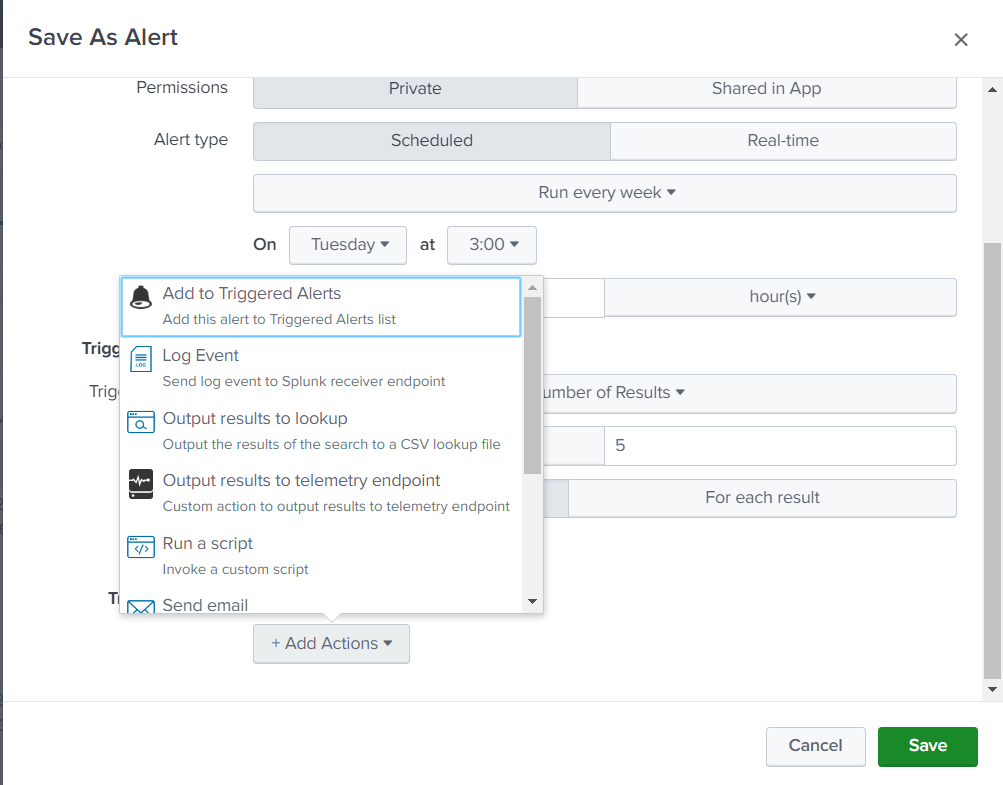
Monitor real-time logs from my machine using splunk



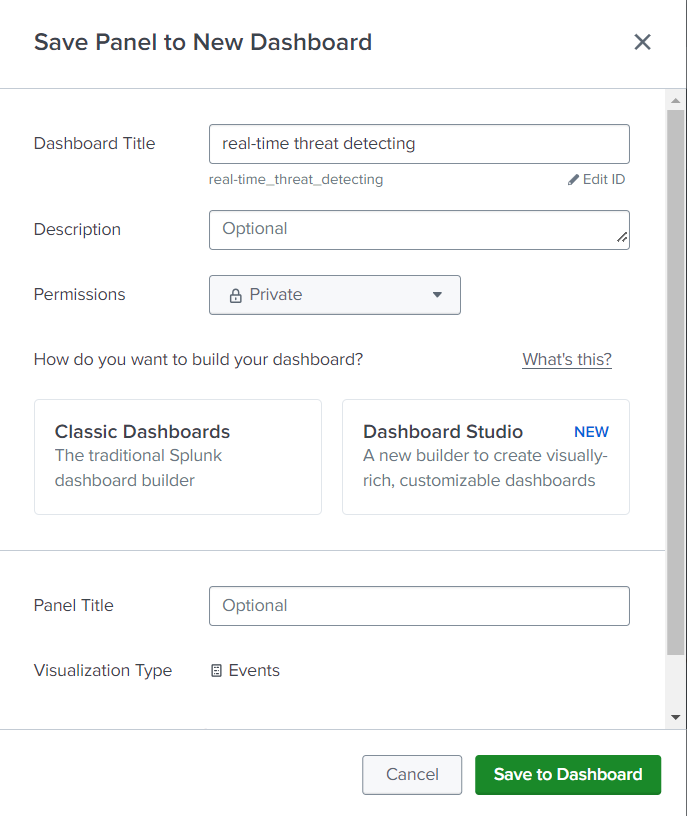
Creating an alert for suspicious activity we searched for the failed logon then we make an alert for it

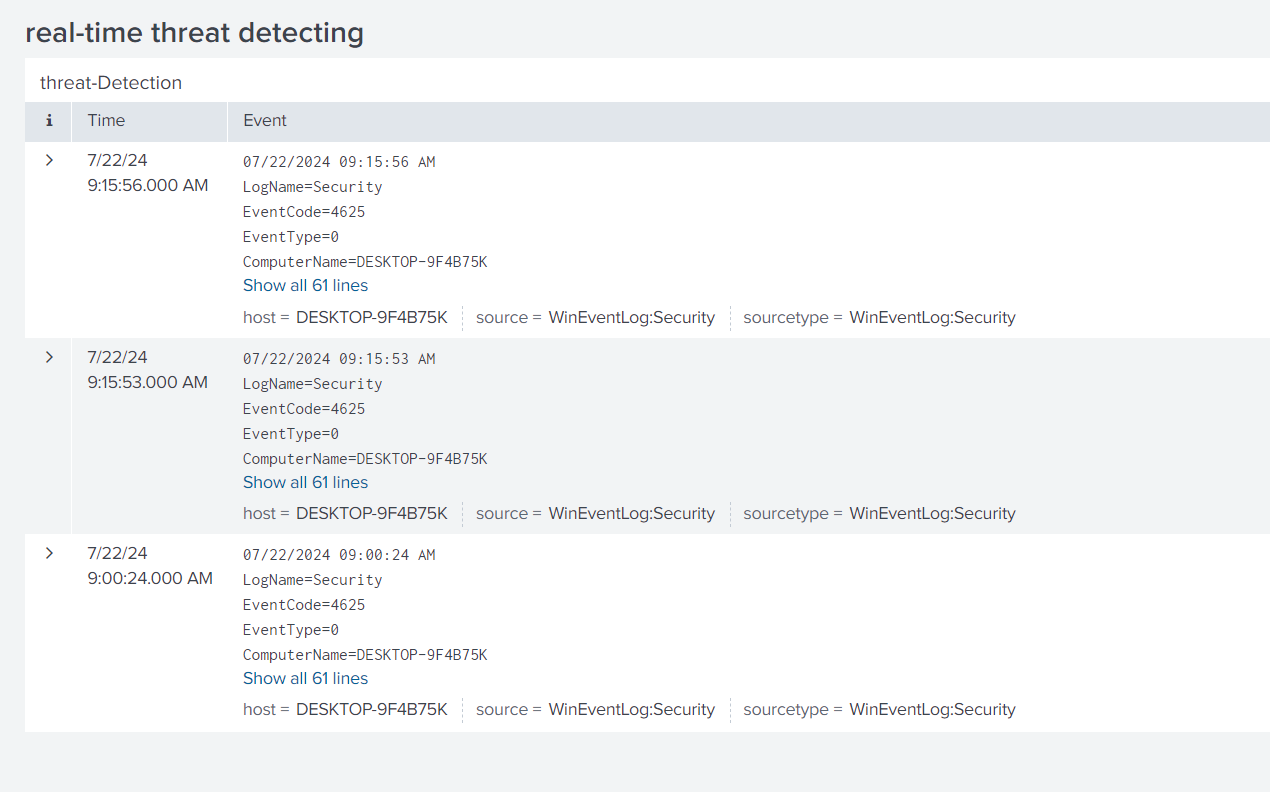
 

Choose the time , when to trigger, what is the action happens after an alert is triggered

we choose to send an email

Making a dashboard for it





eventID = 4625 in windows means failed login to a system