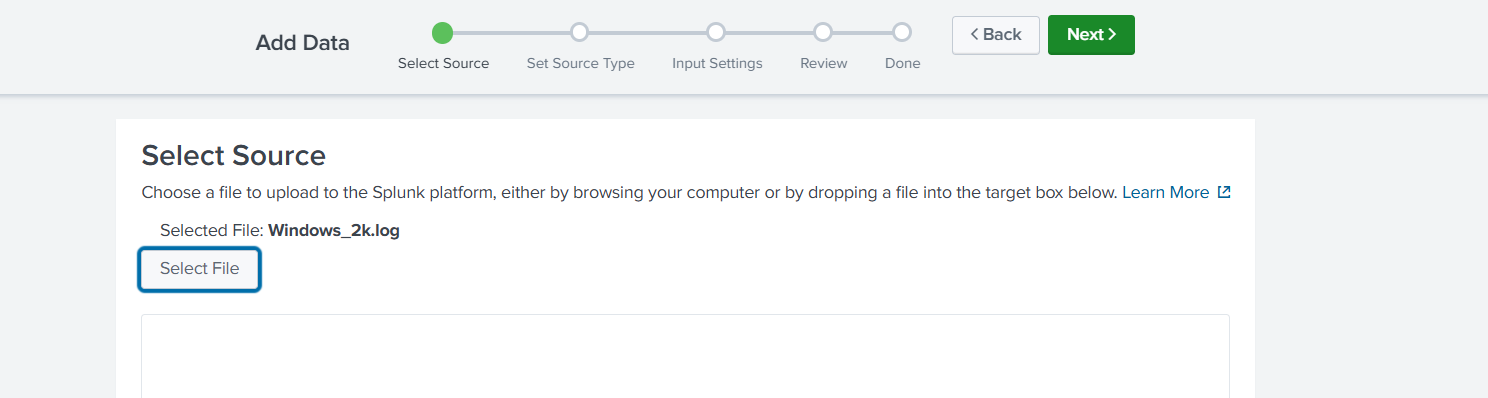
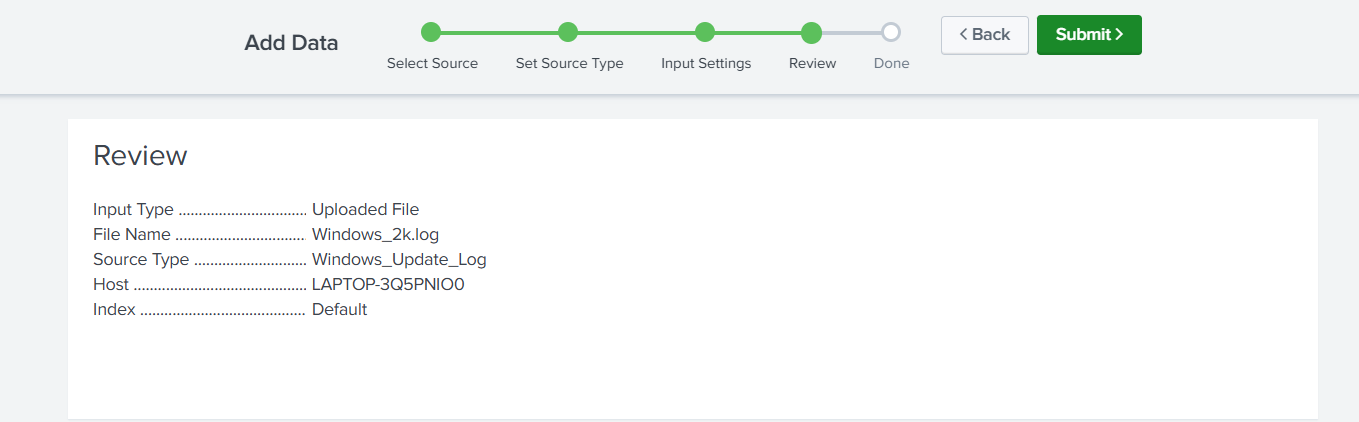
Multi-Line Event Correlation Task using Splunk

Installation of Splunk in windows

Upload dataset in Splunk

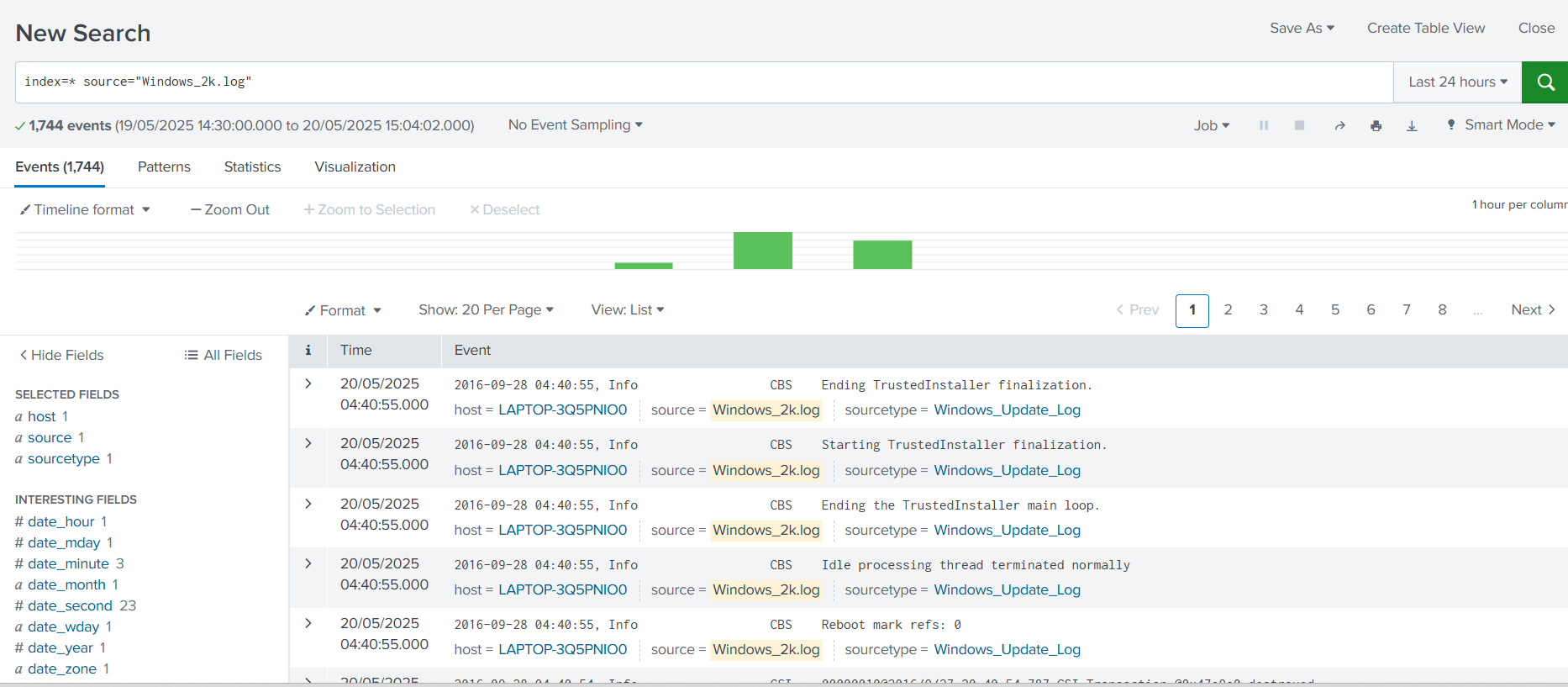


Review check



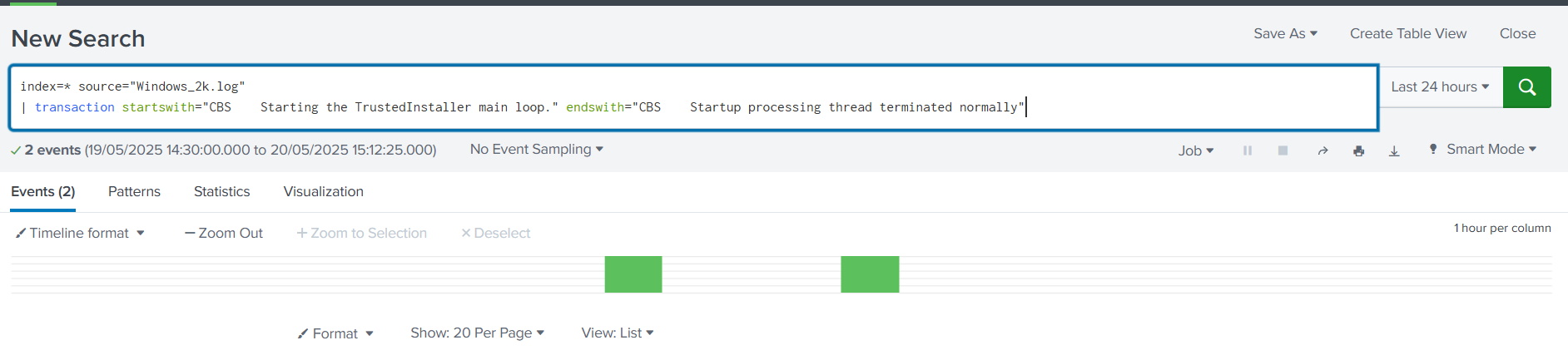
Open Search & Reporting

1. Open your browser and go to: http://localhost:8000  
   2. Login to Splunk Web.  
   3. Click on the 'Search & Reporting' app from the homepage or top menu.



# Run SPL to correlate related events

Paste this SPL in the search bar:  
  
index=\* source="Windows\_2k.log"  
| transaction startswith="CBS Starting the TrustedInstaller main loop." endswith="CBS Startup processing thread terminated normally"  
  
This groups all log lines between the start and end messages into one transaction.



# View full grouped transactions

To see each transaction's duration, line count, and raw content, use:  
  
index=\* source="Windows\_2k.log"  
| transaction startswith="CBS Starting the TrustedInstaller main loop." endswith="CBS Startup processing thread terminated normally"  
| table \_time duration eventcount \_raw  
  
\_time → transaction start time  
duration → how long it took  
eventcount → number of events grouped  
\_raw → full combined log text

