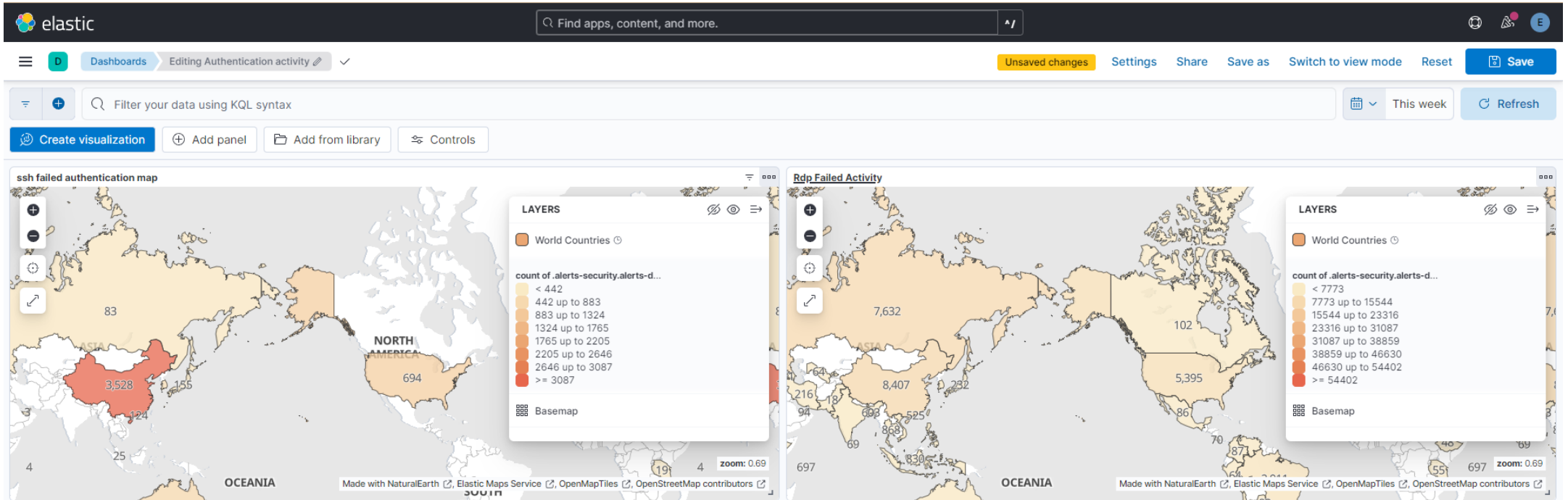
Day 17 - Create Alerts and Dashboards – part 3

Obiettivi

- **Creare una dashboard per l'attività di autenticazione su server tramite RDP e SSH**

Create Alerts and Dashboards

Come nel Day 14 creaiamo una dashboard nella sezione ‘Maps’ per i tentativi di autenticazione falliti sul server **Windows**, salviamo la mappa e la inseriamo nella **Dashboard** creata in precedenza dove abbiamo salvato quella dei tentativi di autenticazione tramite Ssh sul server Ubuntu.



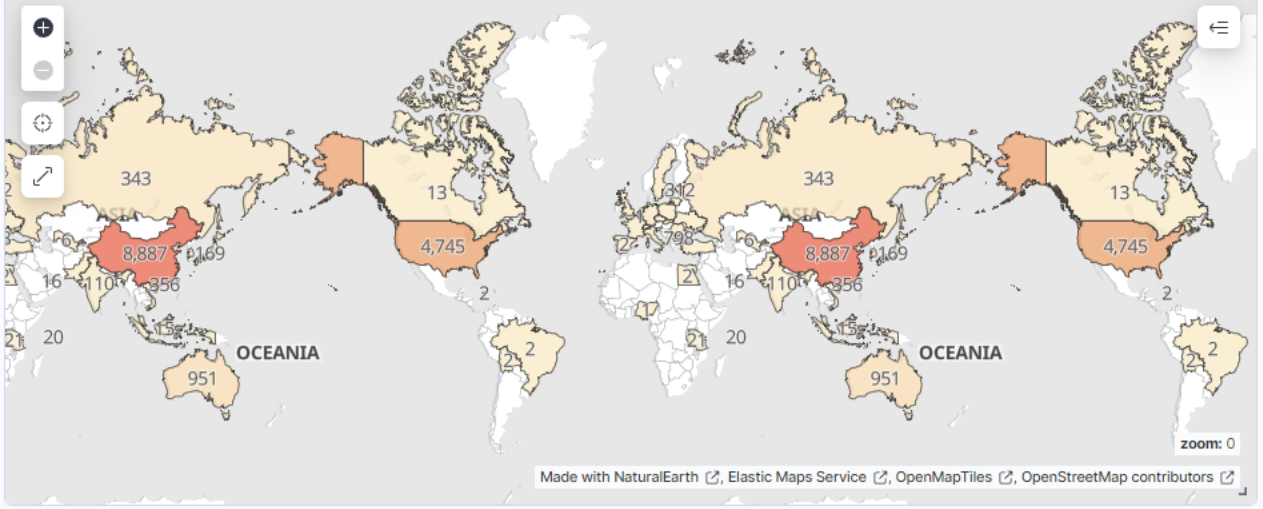
Create Alerts and Dashboards

Ora possiamo aggiungere oltre ai tentativi falliti di autenticazione anche quelli effettuati con successo, tenendo a mente che, per l'event code 4264 in quel caso avremo come logon type 7 e 10.
La query da inserire nel 'Discover' sarà:

```
event.code: 4624 and (winlog.event_data.LogonType : "7" or  winlog.event_data.LogonType : "10")
```

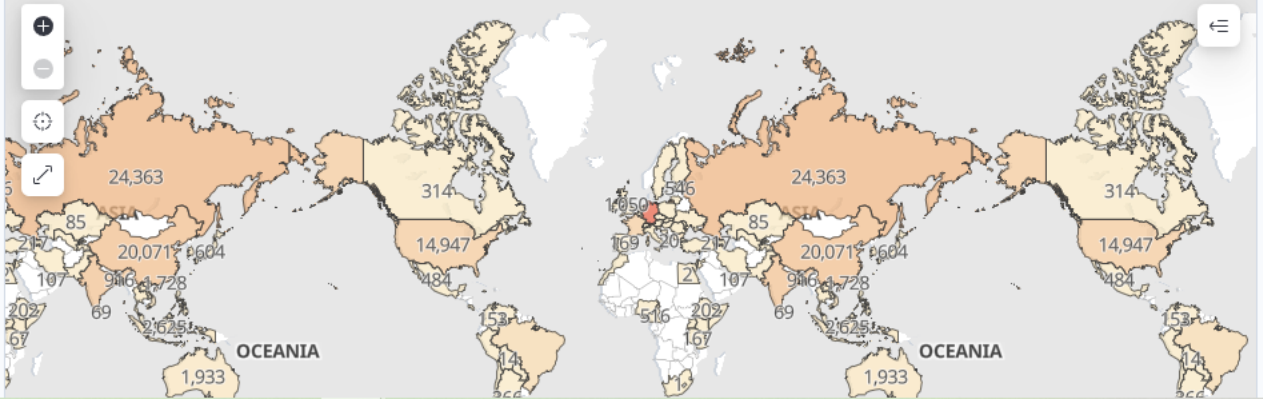
Per creare una mappa con i dati della nuova query entro nella Dashboard , clicco su 'Duplicate' su quella appena creata, cambio la query e avrò un risultato come nella slide successiva.

ssh failed authentication map



ssh successful authentication

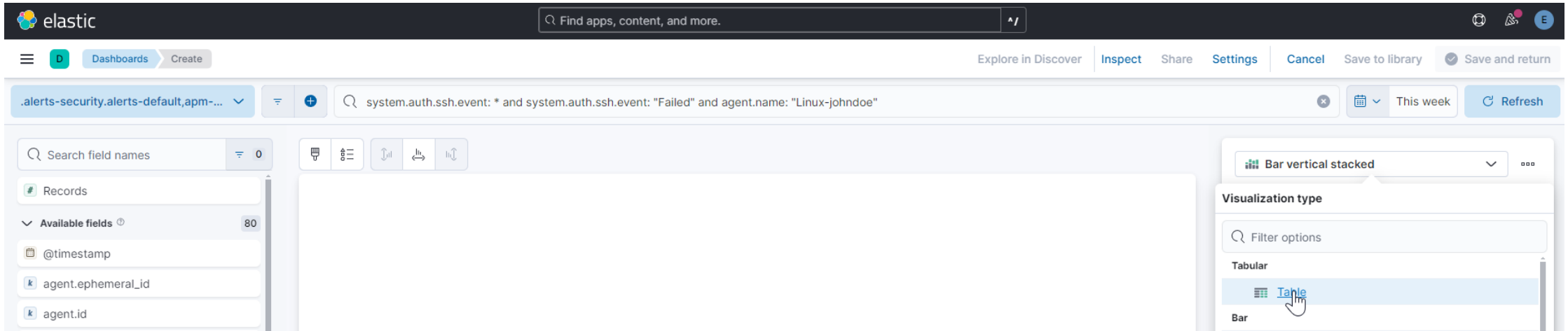
Rdp Failed Activity



Rdp Successful Activity

Create Alerts and Dashboards

Al fine di avere un quadro della situazione più chiaro aggiungiamo alla Dashboard una tabella con i primi 10 risultati di tentativi di autenticazione falliti e riusciti. Dalla Dashboard con le 4 mappe clicchiamo su 'Create Visualization' (in modalità Edit).
Aggiungiamo le query e selezioniamo i campi che ci interessano di quella ricerca: user.name, source.ip, count of records, source.geo.country_name.
In questo caso per ogni campo aumenterò il numero di valori da considerare e deselezionerò 'Group remaining values as "Other"', in modo da visualizzare tutte le entries per quel campo.
Fatto ciò clicco in alto a destra su 'Save and Return'.



Una volta salvato il risultato sarà questo, oltre ad avere la grafica con la mappa avremo una tabella con i dati più rilevanti riassunti. Faremo lo stesso con le autenticazioni **RDP**.