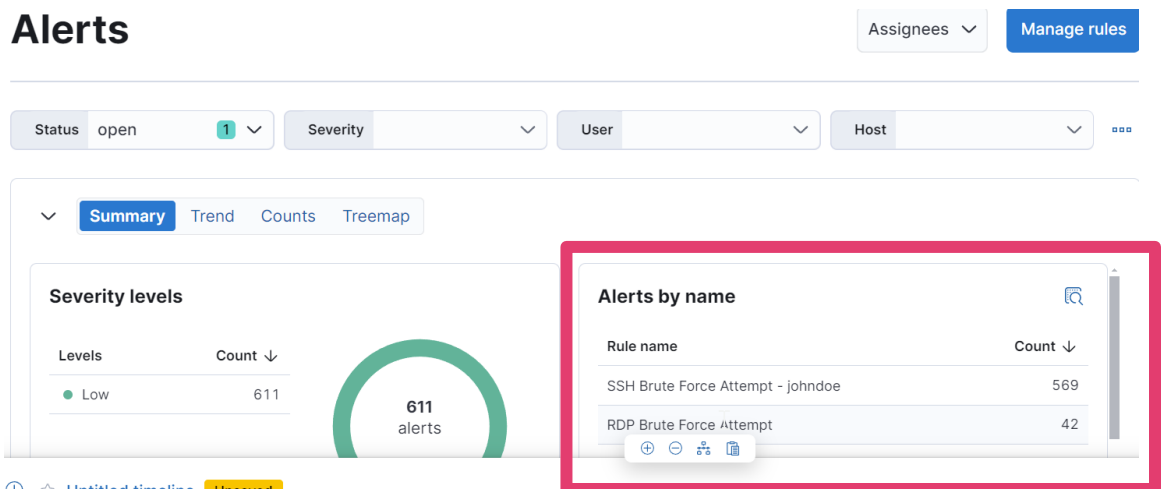
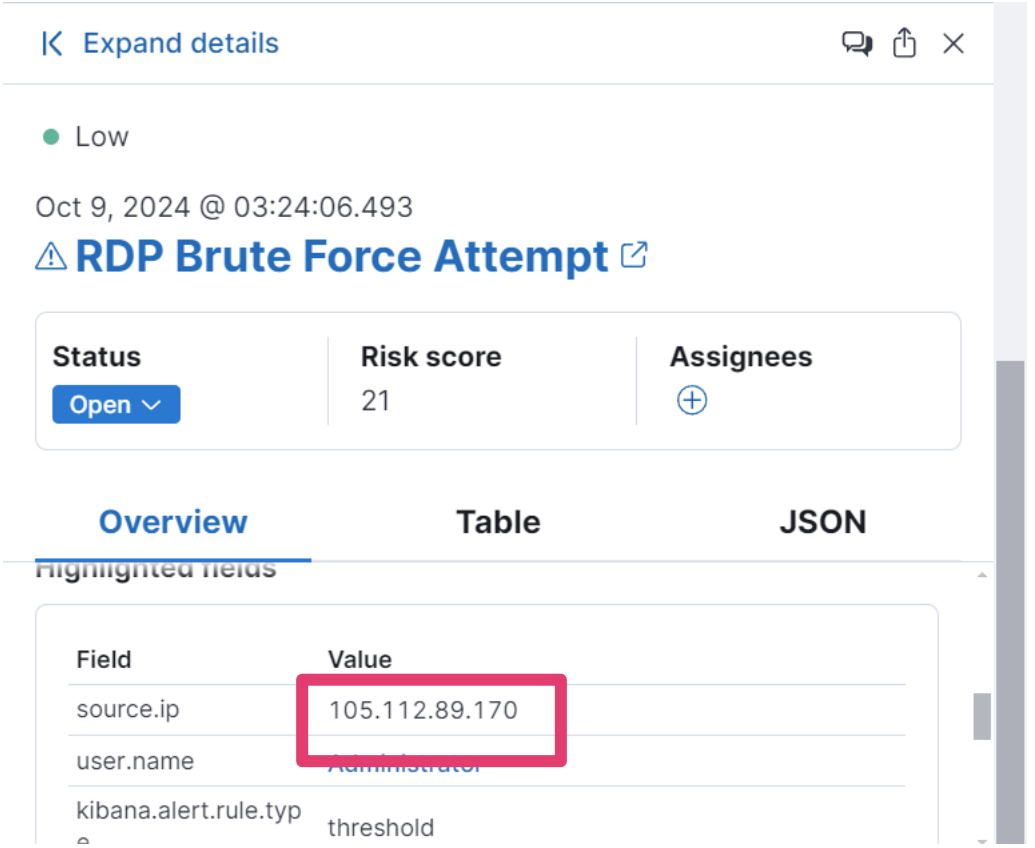
Day 27 -Investigate RDP Brute Force Attack

Investigate RDP Brute Force Attack

Ripetiamo quanto fatto nel Day 26, prendo un alert relativo a un tentativo di Brute Force RDP.
Per farlo nella schermata degli alert clicco su quello che mi interessa.
Anche qui possiamo investigare tramite **abuseipdb e greynoise.**
Procediamo anche qui con la creazione dell'alert da comunicare a osTicket.





Investigate RDP Brute Force Attack

Anche qui modificheremo la regola dell'alert per attacchi RDP nella sezione 'Actions' e la imposteremo come nel Day 26.
Dopo ciò posso effettuare ulteriori indagini per vedere se con questo IP l'utente ha avuto accesso tramite la seguente query:

```
105.112.89.170 and event.code:4624
```

Possiamo inoltre vedere se tale attacco è stato effettuato su più account, in questo ne risultano solo 2.