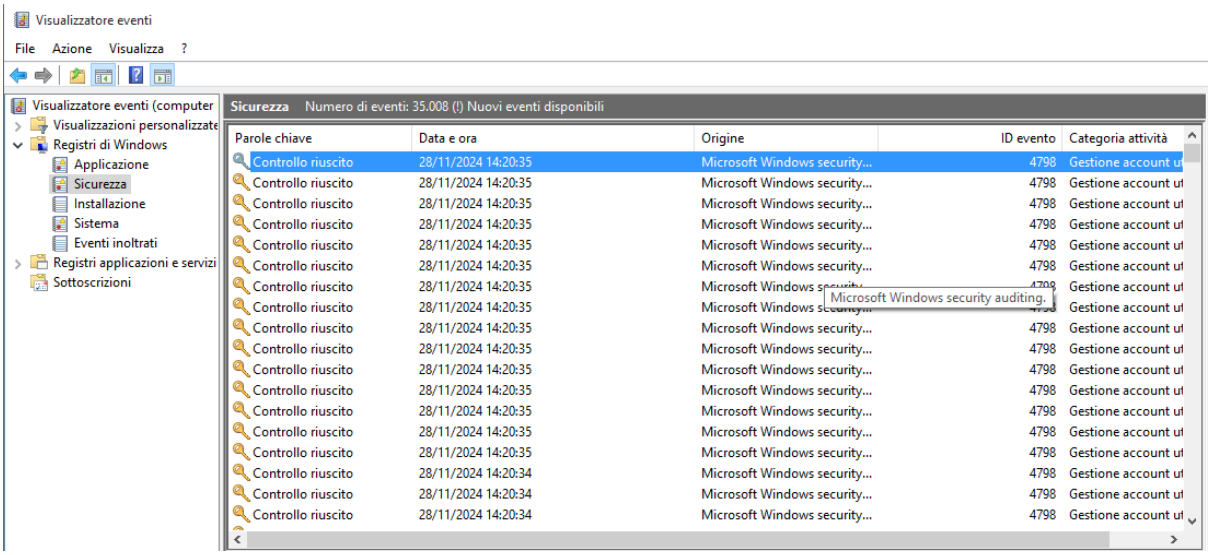
REGISTRI DI SICUREZZA WINDOWS

Nell'esercizio di oggi andremo a visualizzare e configurare regole di log degli eventi di sicurezza windows.

Accediamo tramite comando **win + R** e digitiamo **eventvwr** per accedere al visualizzatore eventi



In questa sezione possiamo vedere tutti i log degli eventi relativi alla sicurezza della nostra macchina *windows*.

In particolare possiamo visualizzare eventi come accessi, tentativi di accesso falliti, modifiche ai privilegi e altre attività critiche.

Inoltre possiamo configurare filtri per visualizzare solo eventi specifici, come quelli relativi a determinati utenti o a determinate attività di sicurezza, esportare i log o configurare allarmi per eventi critici.

Questa pratica ci permette di avere un monitoraggio costante sulla nostra macchina dandoci la possibilità di conseguenza di poter analizzare e agire proattivamente ad un eventuale minaccia.