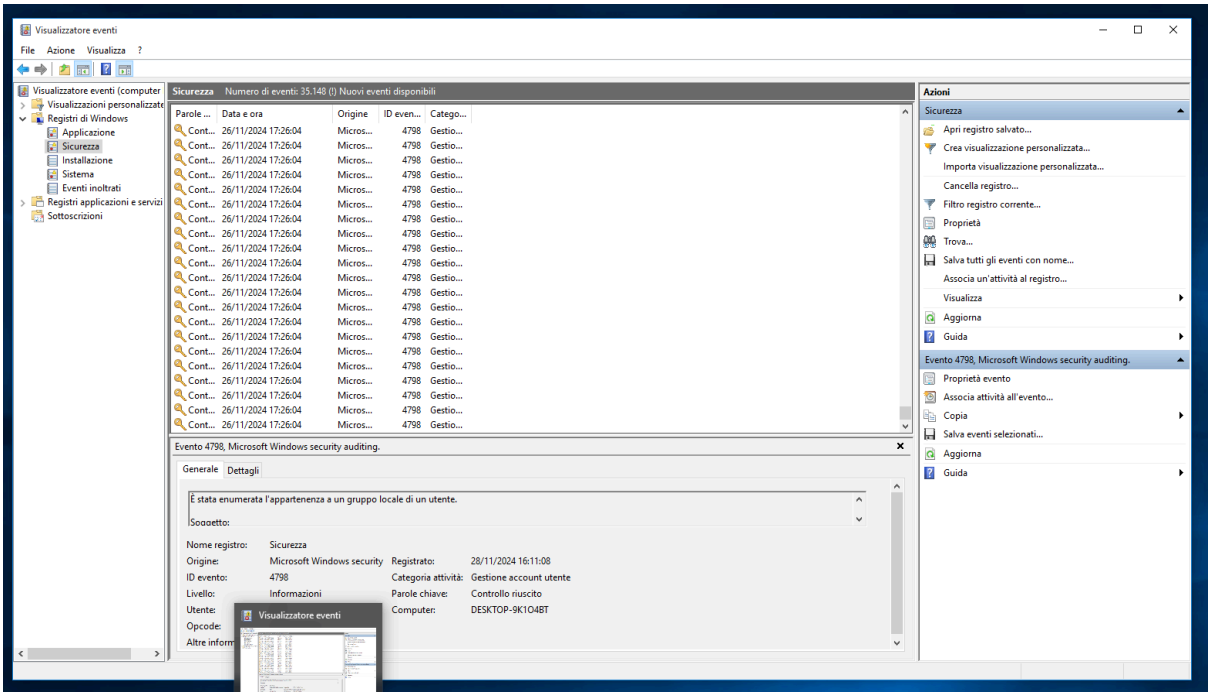
Esercizio S9L4 - Registri di sistema Windows

Durante l'attività odierna, mi sono occupato di analizzare i registri di sicurezza di Windows utilizzando lo strumento "Visualizzatore eventi". L'obiettivo era identificare potenziali anomalie o verificare il normale funzionamento del sistema. Dal controllo effettuato, ho riscontrato un'elevata presenza di eventi con ID **4798**.



Lo screenshot allegato mostra il registro degli eventi di sicurezza. L'ID **4798** si riferisce a un'attività di "Microsoft Windows security auditing", che segnala l'**enumerazione dell'appartenenza a gruppi locali di un utente**. Questo tipo di evento può verificarsi durante normali attività di sistema, come controlli amministrativi o richieste di autenticazione da parte di utenti o servizi. Tuttavia, un volume elevato di questi eventi potrebbe indicare attività sospette, come tentativi non autorizzati di verificare privilegi.

L'analisi non evidenzia anomalie significative, ma è consigliabile monitorare regolarmente il sistema e verificare che i processi che generano questi eventi siano legittimi, per garantire la sicurezza del sistema.