Analisi dei Registri di Sicurezza

- **Data Analisi:** 05 Febbraio 2026

1) Introduzione e obiettivo

Il presente documento analizza l'attività del sistema operativo Windows rilevata tramite lo strumento **Visualizzatore Eventi** (Event Viewer). L'analisi si concentra sul registro di **Sicurezza**, il quale monitora i tentativi di accesso, l'uso dei privilegi di sistema e le attività delle sessioni utente.

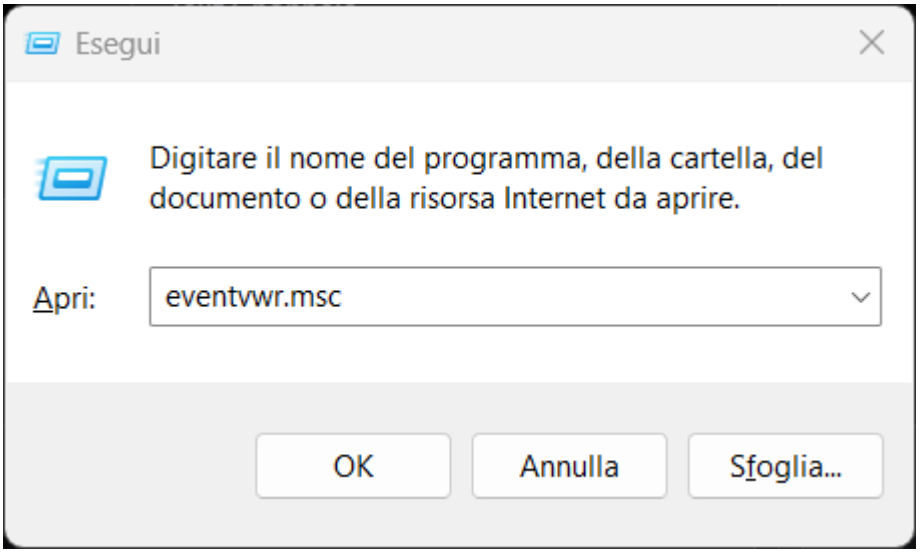
L'obiettivo di questo report è identificare la natura di una serie di eventi ad alta frequenza che coinvolgono la creazione e la terminazione di sessioni di login, al fine di distinguere tra i normali processi automatizzati del sistema operativo e potenziali anomalie o attività non autorizzate.

2) Sintesi dell'Attività Rilevata

L'immagine mostra una sequenza densa di eventi di **Audit Success** (Successo del controllo) che si ripetono con una frequenza estremamente elevata (diversi eventi al secondo).

Comandi usati:

- ***`win + r`***
- ***`eventvwr.msc`***
- ***`win + l`***

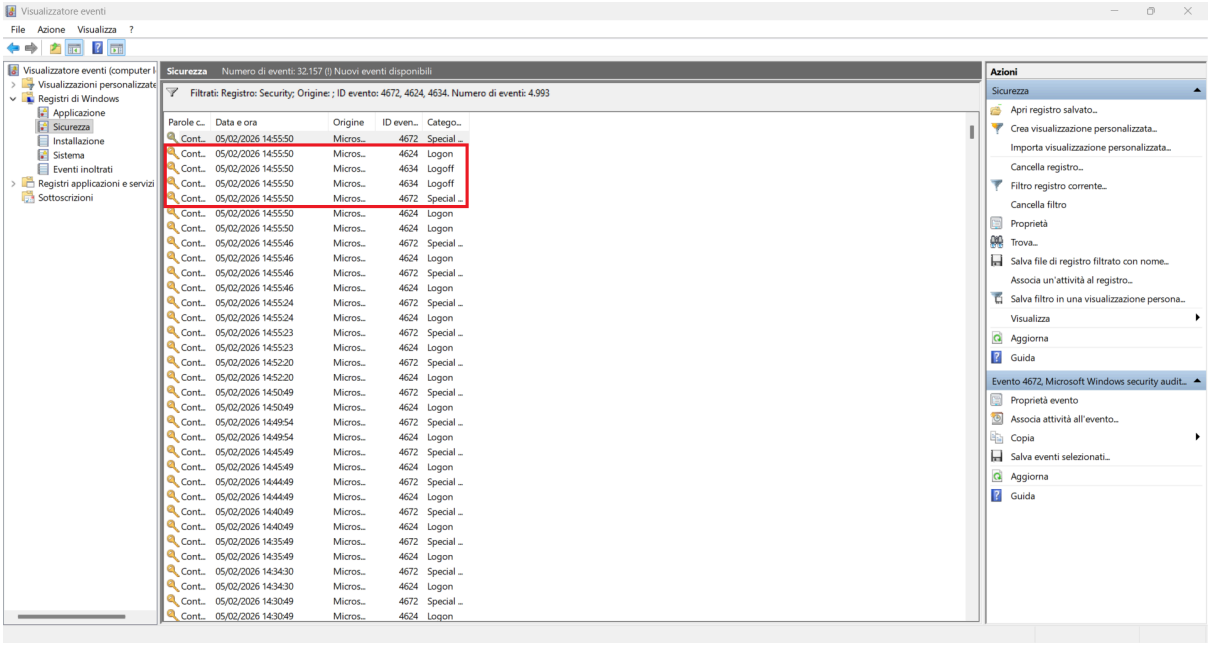


Analisi degli ID Evento (Event ID):

Dallo screenshot si leggono chiaramente tre codici fondamentali per la sicurezza Windows:

- **ID 4624 (Log on):** Indica che un account ha effettuato l'accesso correttamente.
- **ID 4634 (Log Off):** Indica che una sessione di accesso è stata terminata.

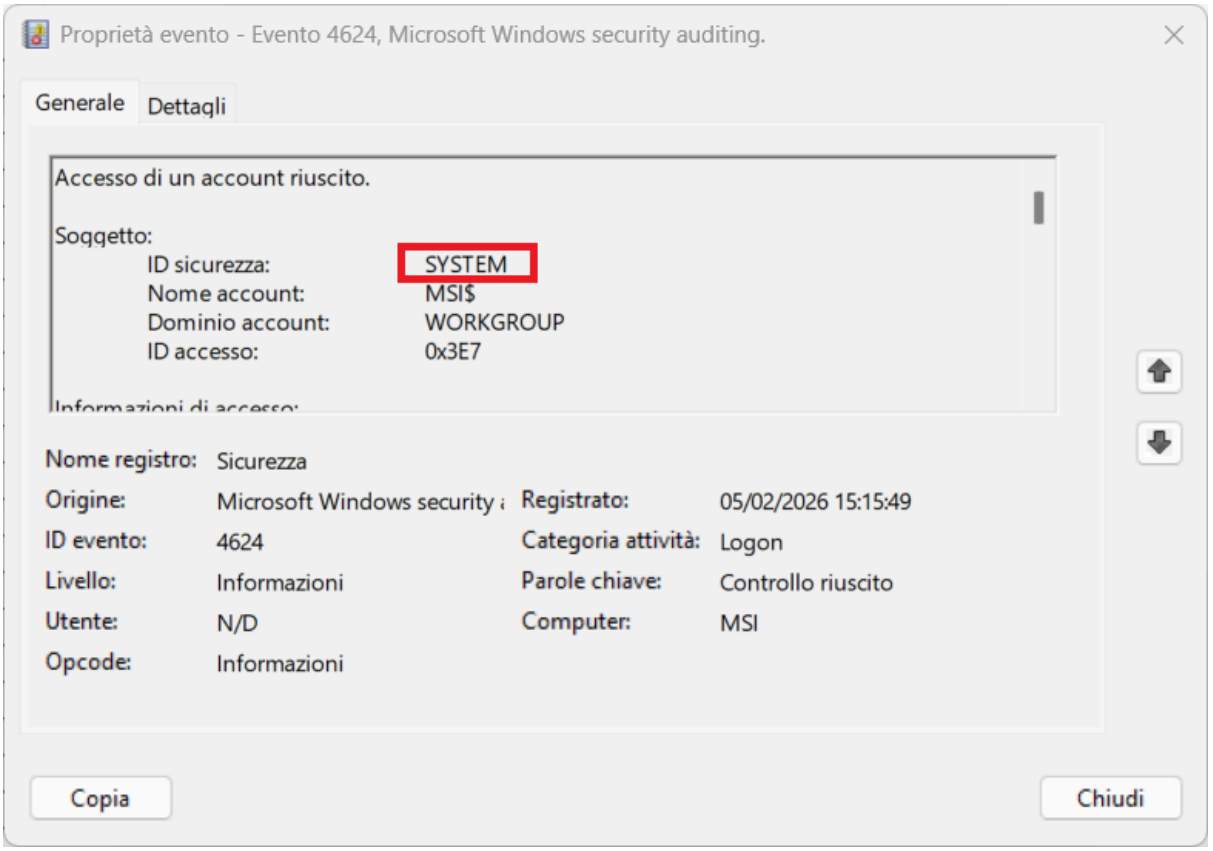
- **ID 4672 (Special Logon):** Indica che sono stati assegnati privilegi "speciali" (amministrativi) a una nuova sessione di accesso. Questo accade quasi sempre quando si accede ad un account con diritti di Administrator.



3) Dettagli Critici (Da verificare)

Per rendere questo report completo, dovresti cliccare su uno degli eventi **4624** o **4672** e guardare il pannello inferiore (Generale). I dati fondamentali da cercare sono:

- **Tipo di accesso (Logon Type):**
  - **-Tipo 2:** Accesso locale (qualcuno alla tastiera).
  - **-Tipo 3:** Accesso via rete (cartelle condivise, stampanti).
  - **-Tipo 5:** Servizio (un servizio di Windows che si avvia).
  - **-Tipo 7:** Sblocco workstation.
- **Nome Account:** Verifica se l'account è *SYSTEM, LOCAL SERVICE* o il tuo nome utente.
- **Processo di origine:** Identifica quale file *.exe* sta generando la richiesta.



4) Valutazione della Sicurezza

- **È un attacco?** Se il "Tipo di Accesso" è **3** e non riconosci l'indirizzo IP sorgente, potrebbe trattarsi di un tentativo di movimento laterale o forza bruta.
- **È un errore?** Se gli eventi riguardano un account locale e il tipo di accesso è **5** o **0**, è molto probabile che sia un comportamento standard di Windows o di un software installato (come un driver o un agent di backup) che lavora in background.