# S9 – L4

## Titolo:

### Analisi e configurazione dei log di sicurezza su Windows

---

## Introduzione:

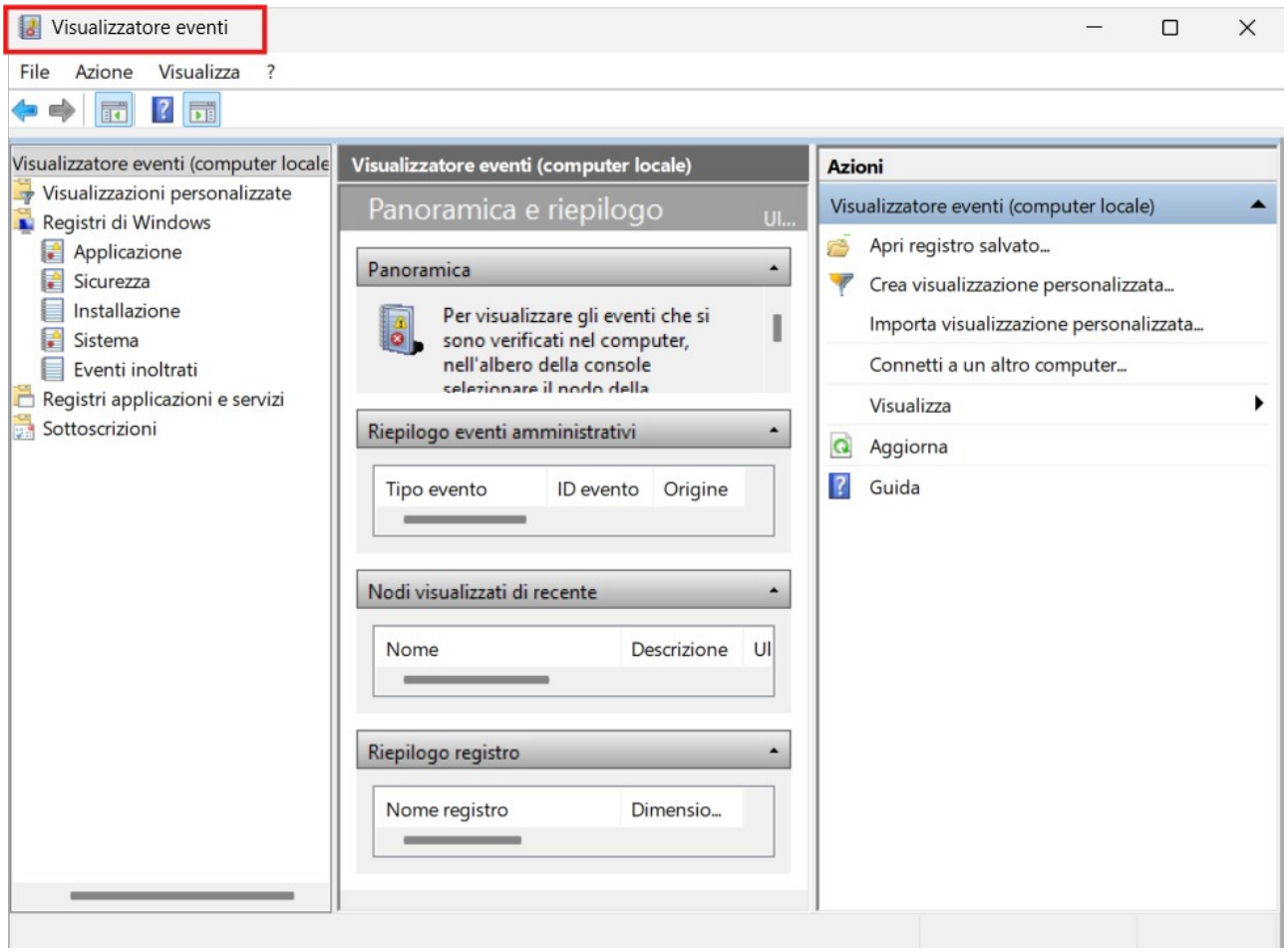
Configuro e analizzo i **log di sicurezza di Windows** utilizzando il **Visualizzatore eventi**, con l'obiettivo di verificare la corretta registrazione degli eventi di **Login e Logoff**. L'attività riproduce una fase fondamentale del monitoraggio della sicurezza, **utile per il rilevamento di accessi legittimi e tentativi di autenticazione falliti.**

---

## Svolgimento dell'esercizio:

### 1) Apertura del Visualizzatore eventi

- **Premo** `Win + R`
- **Digito** `eventvwr`
- **Premo** Invio

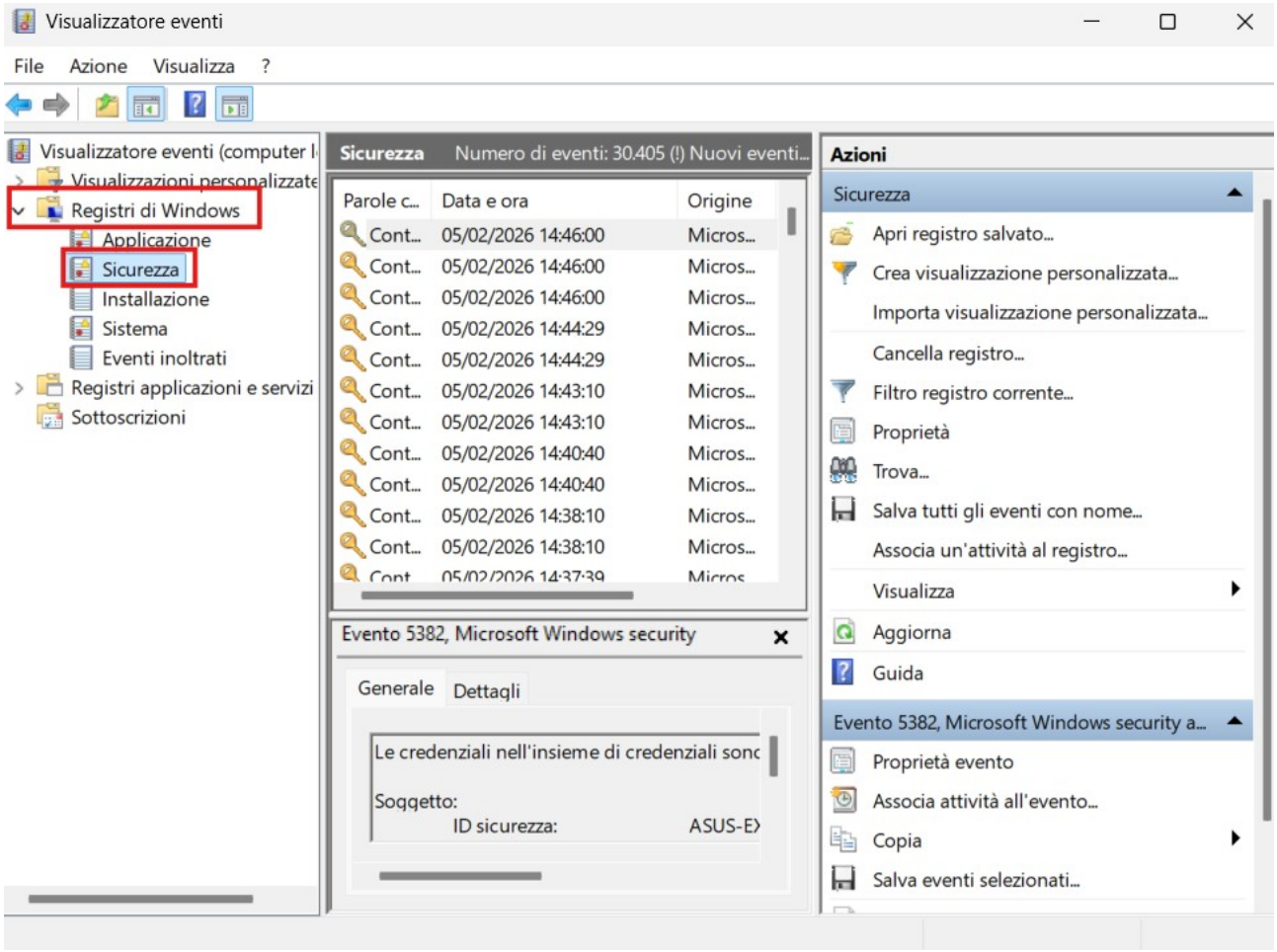


Il Visualizzatore eventi si apre correttamente.

---

## 2) Accesso al registro di Sicurezza

- Nel pannello sinistro **espando** `Registri di Windows`
- **Clicco** su `Sicurezza`

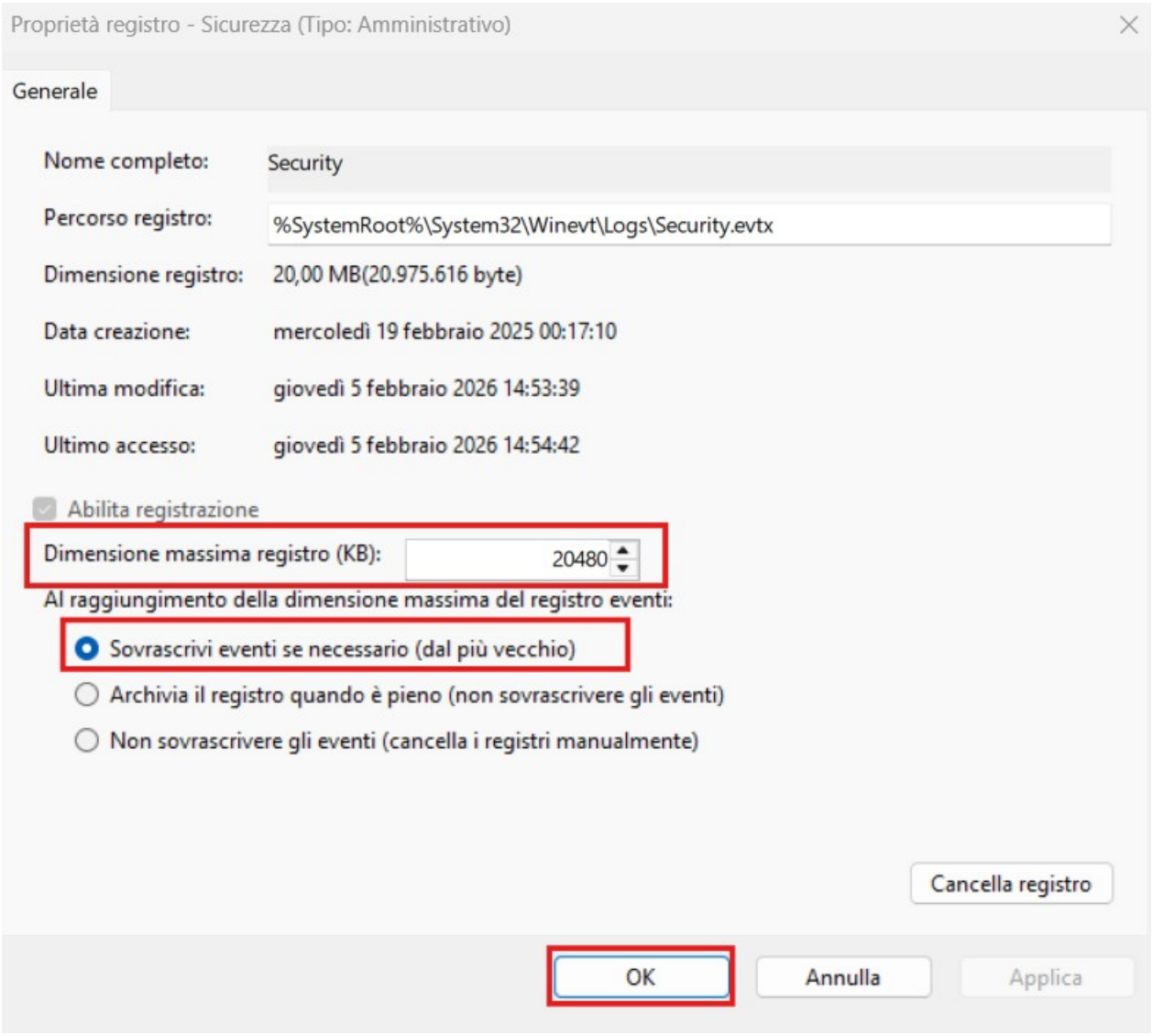



Visualizzo l’elenco degli eventi di sicurezza del sistema.

---

## 3) Configurazione delle proprietà del log Sicurezza

- **Clicco con il tasto destro** su `Sicurezza`
- **Seleziono** `Proprietà`
- **Imposto** una dimensione adeguata del log
- **Seleziono** l’opzione di gestione degli eventi (sovrascrittura/archiviazione)
- **Clicco** su `Applica` e poi su `OK`

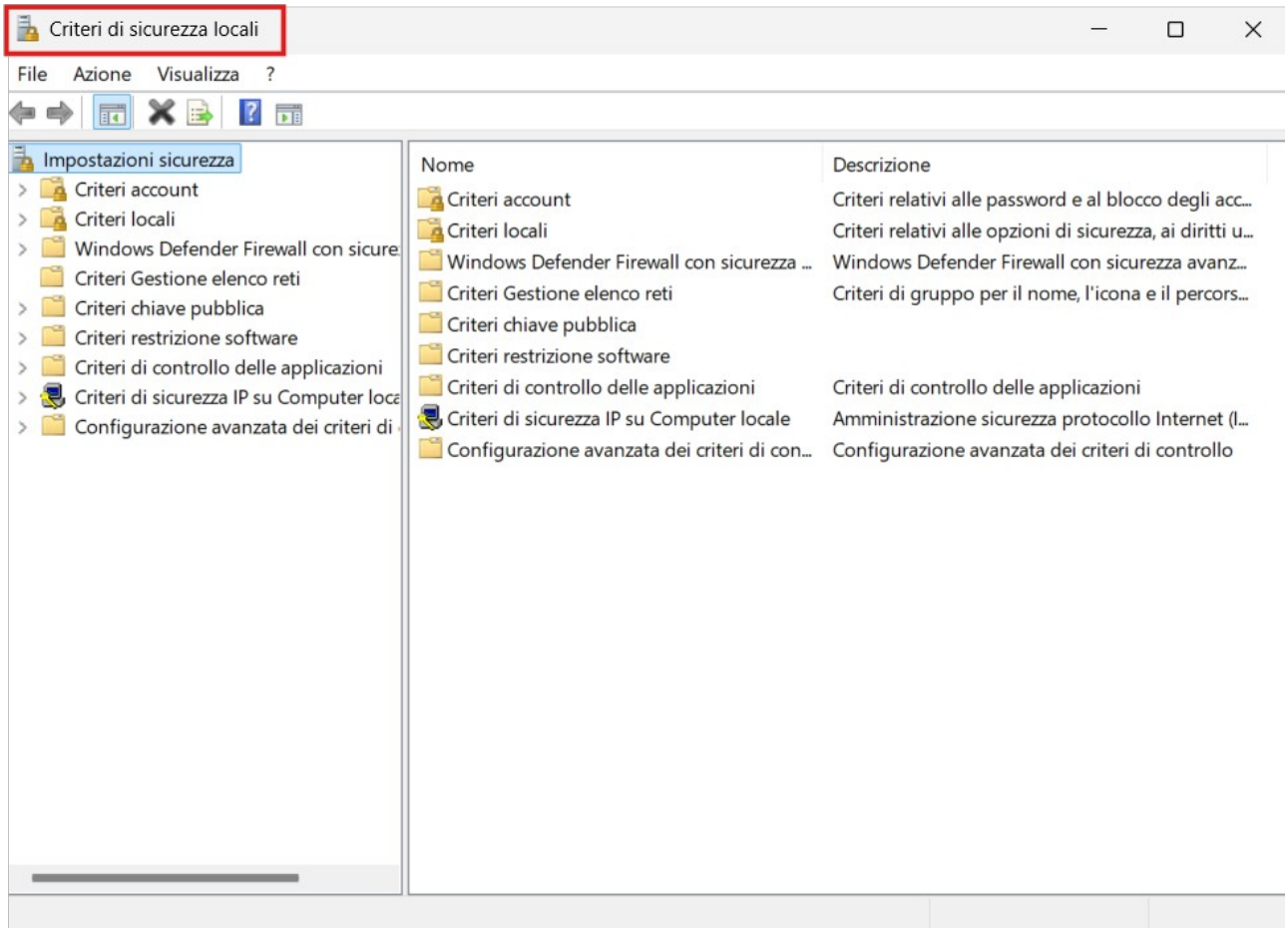



Il log di sicurezza è ora correttamente configurato.

---

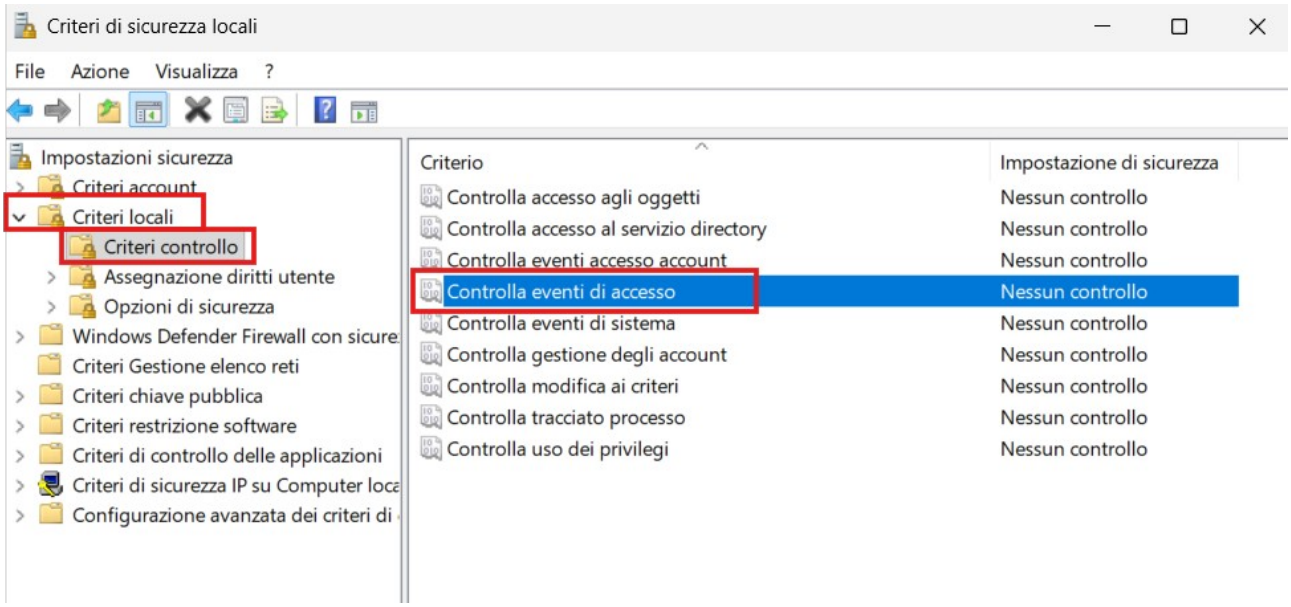
## 4) Abilitazione del logging di Login e Logoff

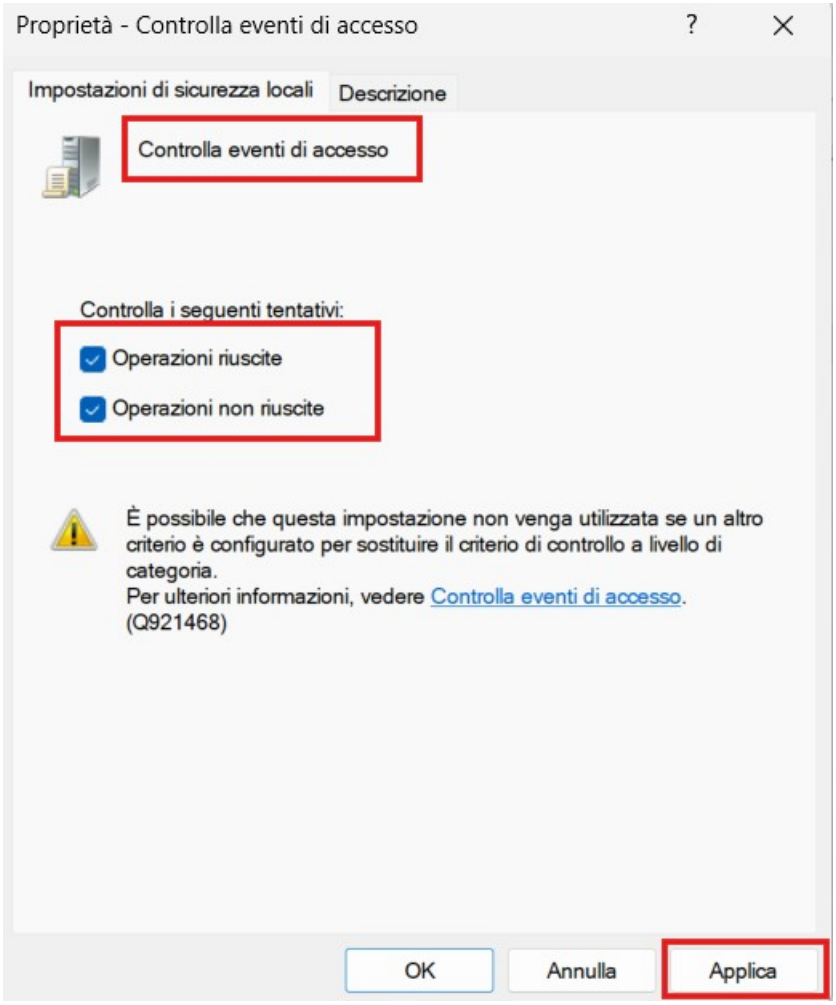
- **Premo** `Win + R`
- **Digito** `secpol.msc`
- **Premo** Invio




Dal pannello:

- **Clicco** su `Criteri locali` → `Criteri di controllo`
- **Apro** `Controlla eventi di accesso (Audit logon events)`
- **Seleziono** `Successo` e `Errore`
- **Applico** le modifiche






In questo modo abilito la registrazione degli eventi di accesso riusciti e falliti.

---

## 5) Generazione di eventi di test

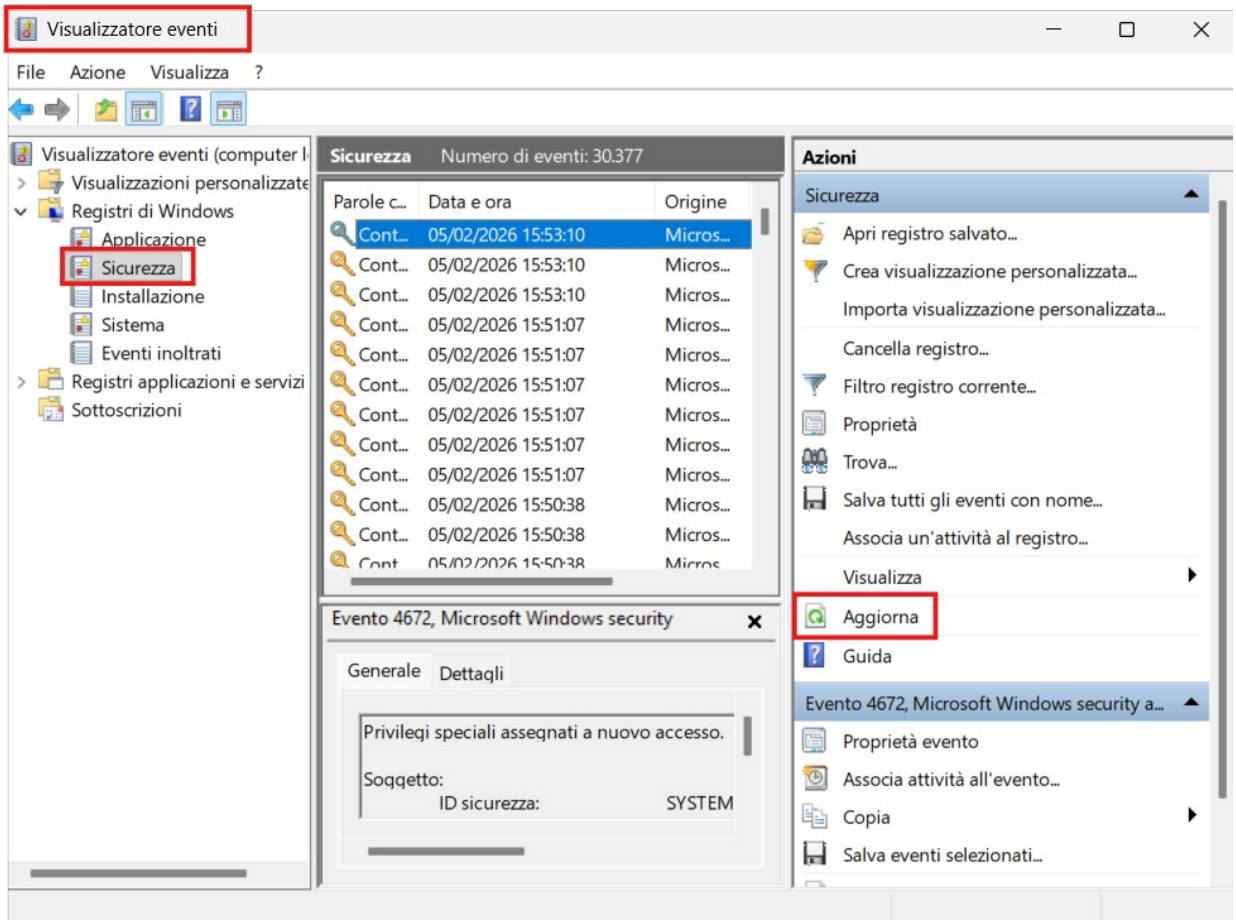
- **Blocco** il computer con `Win + L`
- **Eseguo** un login corretto
- **Eseguo** un tentativo di login errato
- (facoltativo) **Eseguo** il logoff dell'utente

Genero così eventi reali da analizzare
**Screenshot non disponibile per combinazione di tasti non possibile in schermata di login**

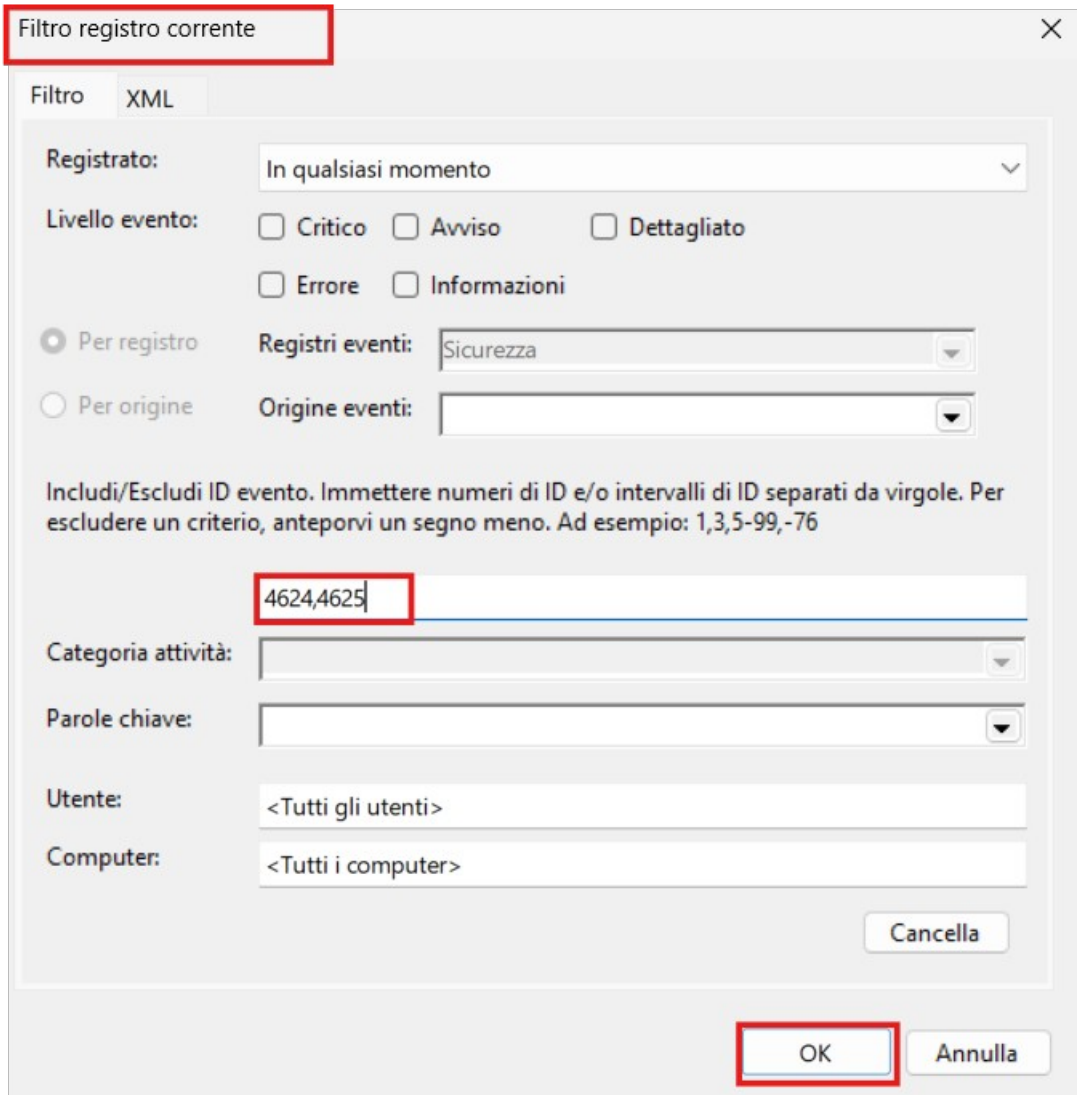
---

## 6) Verifica degli eventi nel registro Sicurezza

- **Torno** nel Visualizzatore eventi
- **Clicco** su `Sicurezza`
- **Aggiorno** il registro

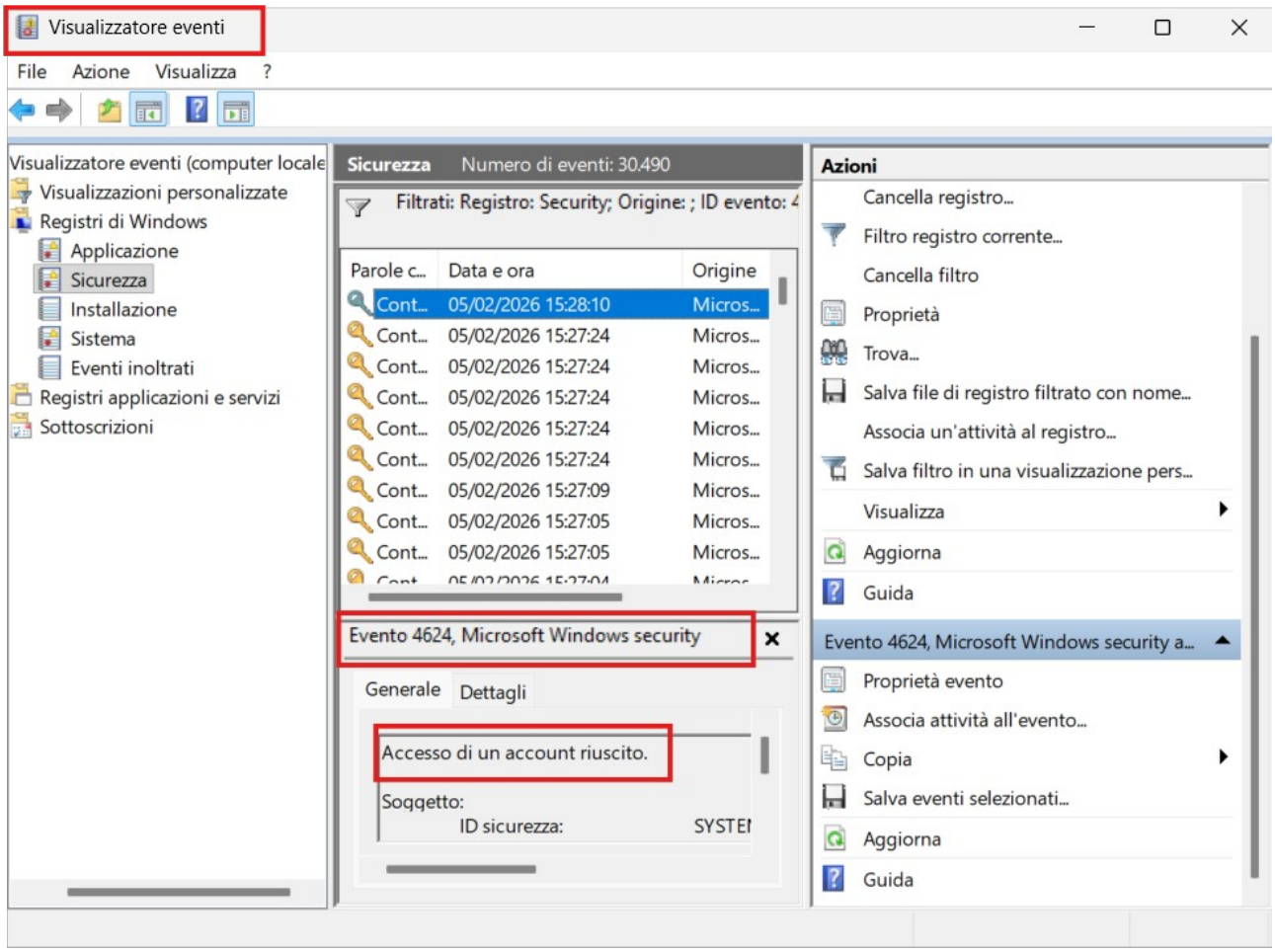


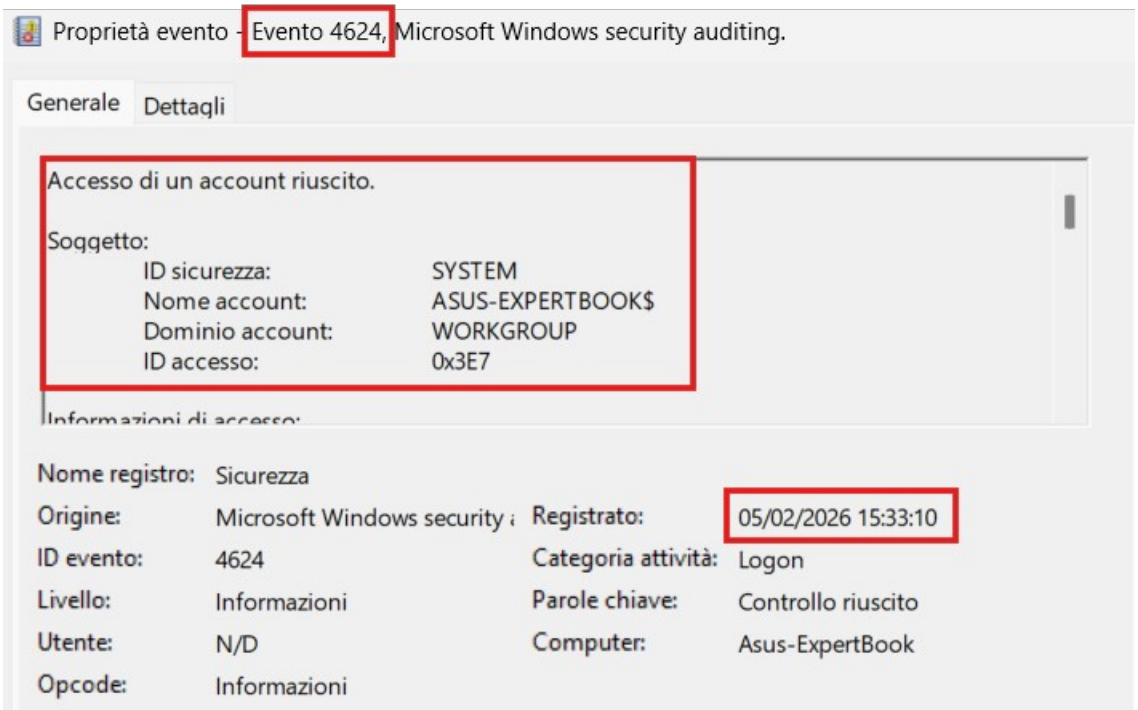
- **Filtro** gli eventi per ID: **4624,4625** (uno alla volta)



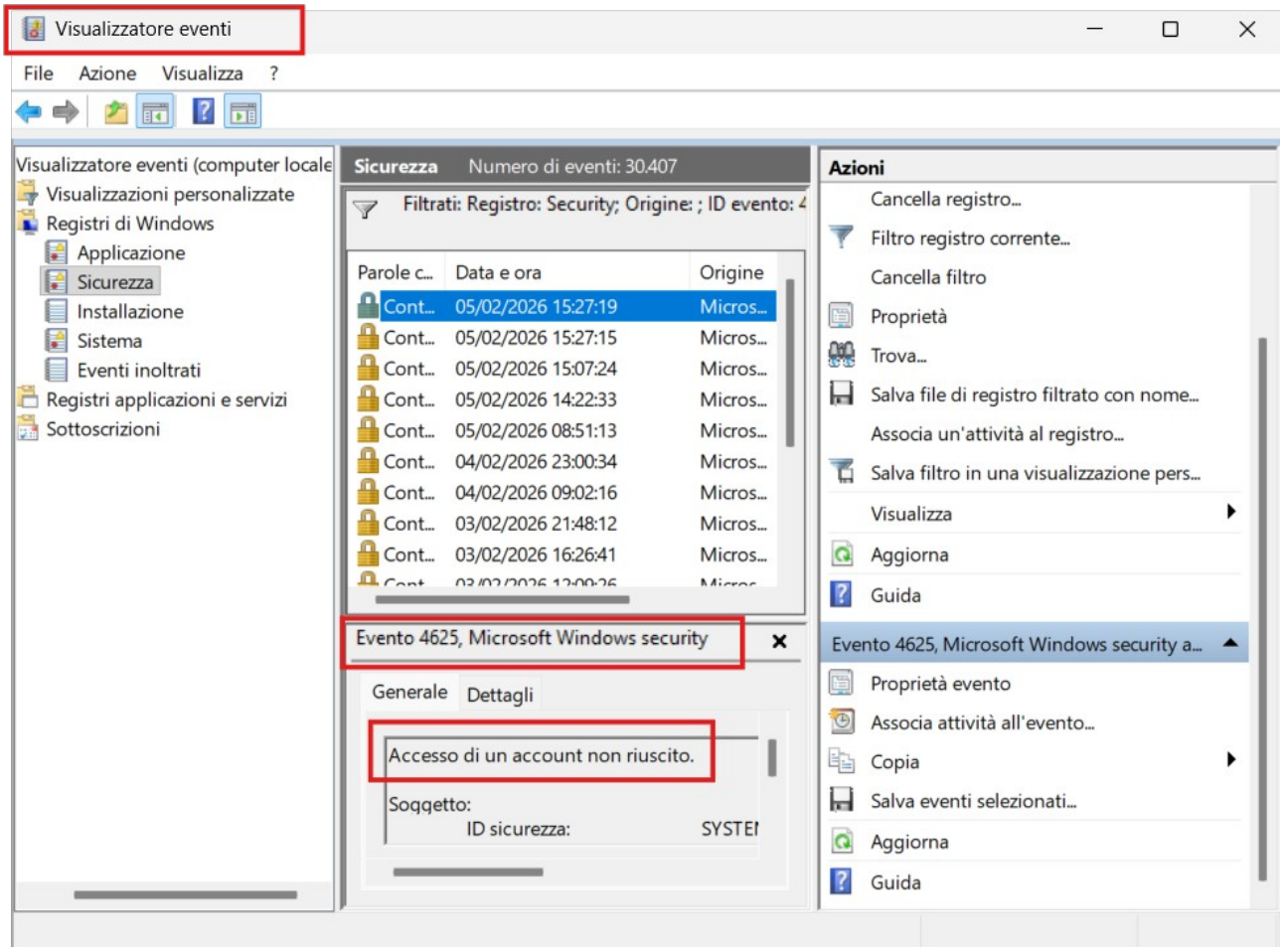

**NB**: si raccomanda di inserire gli ID evento **uno alla volta**, applicando il filtro separatamente per ciascun ID, al fine di evitare che il sistema non visualizzi correttamente tutti gli eventi richiesti quando vengono inseriti contemporaneamente.

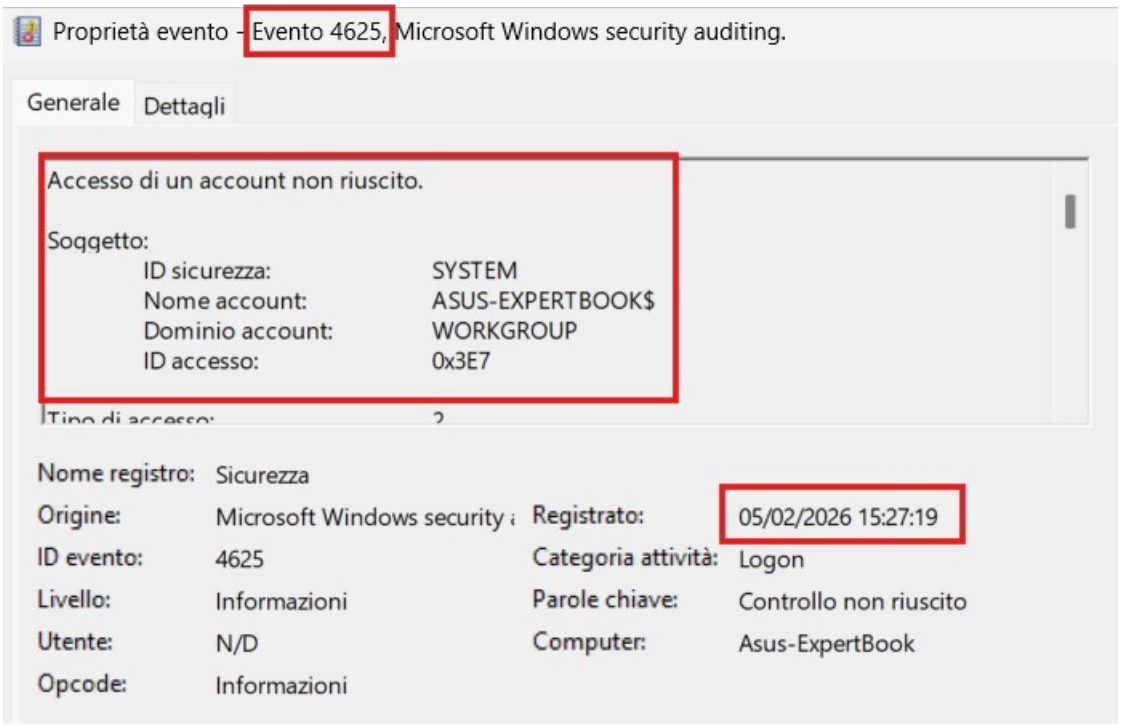
- 4624 → accesso riuscito



- 4625 → accesso fallito



Ho verificato correttamente la presenza degli eventi generati.

---

# Conclusioni ultime:

L’esercizio ha consentito di **configurare e verificare correttamente il registro di sicurezza di Windows, assicurando la registrazione degli eventi di Login e Logoff.**

Attraverso l’**analisi degli ID evento 4624 e 4625** è stato possibile confermare il corretto funzionamento del sistema di auditing locale, d**imostrando come i log rappresentino uno strumento fondamentale per il monitoraggio degli accessi** e per le attività di sicurezza e analisi degli incidenti.