

Report Configurazione e Analisi dei Log di Sicurezza Windows

Data: 05/02/2026

Autore: Nicola Cassandra

Oggetto: Implementazione di regole di monitoraggio per eventi di accesso (Login/Logoff)

1. Introduzione: Creazione e Gestione delle Regole di Log

La gestione efficace dei file di log (Log Management) è il primo pilastro della difesa informatica e della risposta agli incidenti. Windows registra nativamente ogni attività nel **Visualizzatore Eventi** (Event Viewer), ma la mole di dati grezzi rende spesso impossibile un'analisi manuale efficace.

La creazione di **Regole di Filtraggio** non è una semplice operazione di pulizia, ma una strategia difensiva che permette di:

- **Isolare anomalie:** Distinguere il comportamento normale da tentativi di intrusione.
- **Ottimizzare i tempi di risposta:** Permettere agli analisti di concentrarsi solo su eventi che richiedono attenzione (es. accessi falliti).
- **Garantire la Non-Repudiation:** Tracciare con certezza chi ha fatto cosa e quando.

Nel contesto di questo esercizio, ci siamo concentrati sulla creazione di una "vista personalizzata" focalizzata esclusivamente sul ciclo di vita della sessione utente (Entrata/Uscita).

2. Analisi dello Stato Iniziale

Dall'analisi preliminare del sistema, il registro di sicurezza presentava una saturazione di eventi eterogenei.

- **Volume Dati:** Il contatore totale segnava **24.245 eventi**.
- **Tipologia Eventi:** Erano visibili numerosi eventi di sistema non critici per l'analisi degli accessi, come l'ID **5061** (Operazione crittografica), l'ID **5379** (Gestione credenziali/User Account Management) e l'ID **4672** (Assegnazione privilegi speciali).
- **Criticità:** In questo stato, individuare un tentativo di accesso illegittimo (Brute Force) sarebbe risultato estremamente complesso a causa dell'eccessivo rumore di fondo.

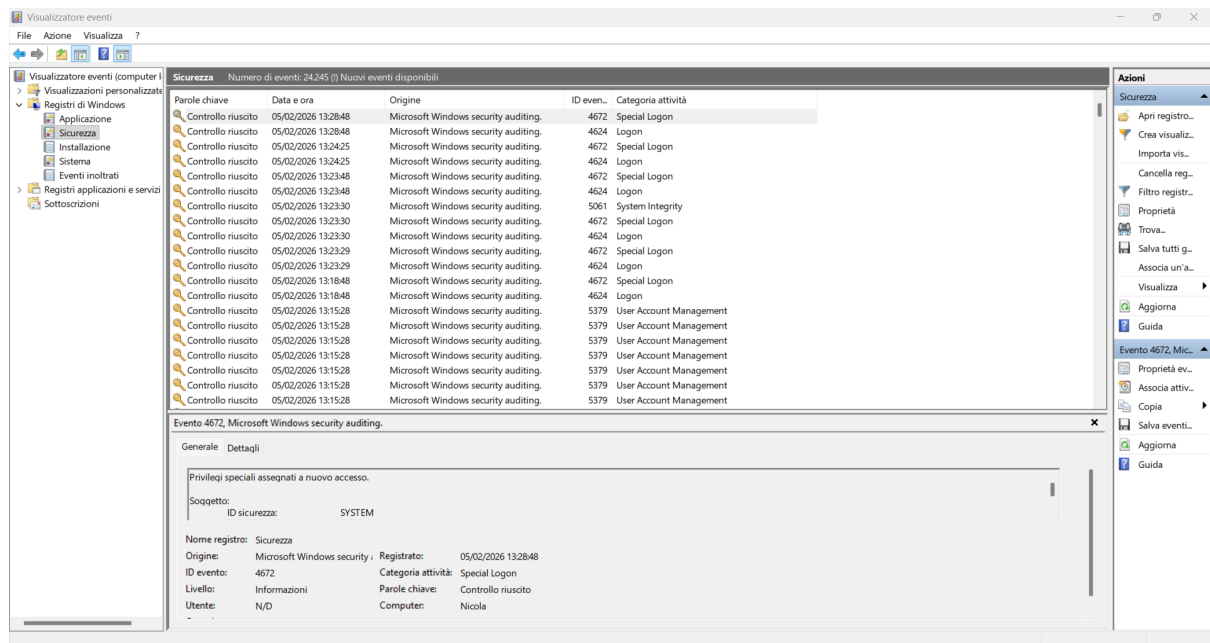


Figura 1: Panoramica iniziale del registro 'Sicurezza' (Security Log). Lo screenshot evidenzia la saturazione del registro con oltre 24.000 eventi generici. Si noti la presenza di "rumore di fondo" costituito da eventi di sistema (es. ID 5061, 5379) che rendono complessa l'individuazione immediata degli accessi utente.

3. Metodologia di Implementazione

Per strutturare il monitoraggio, è stata utilizzata la funzione "Filtro registro corrente" del Visualizzatore Eventi.

3.1 Definizione dei Parametri

È stata configurata una regola di filtraggio basata sugli ID Evento standard per l'auditing di Windows. La configurazione applicata è stata la seguente:

- **Target:** Registro "Sicurezza".
- **ID Evento Selezionati:** 4624, 4625, 4634, 4647.

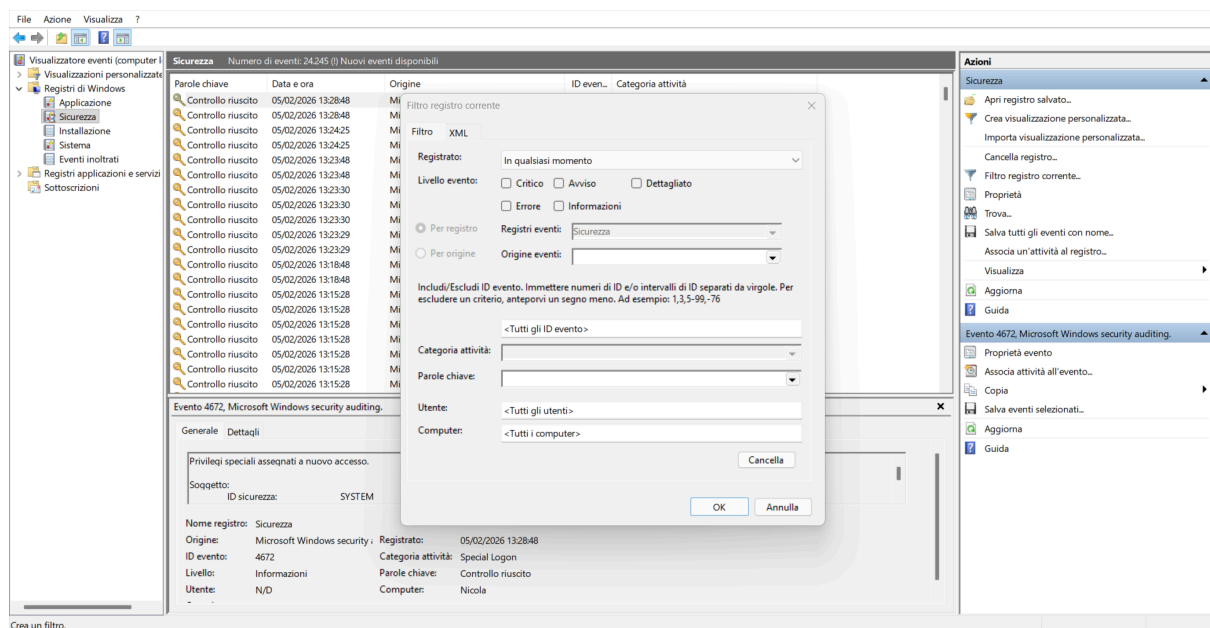


Figura 2: Interfaccia di configurazione del filtro. Accesso al menu "Filtro registro corrente". Questa funzionalità permette di creare una vista logica sui dati senza alterare o cancellare i log originali, garantendo l'integrità forense delle prove.

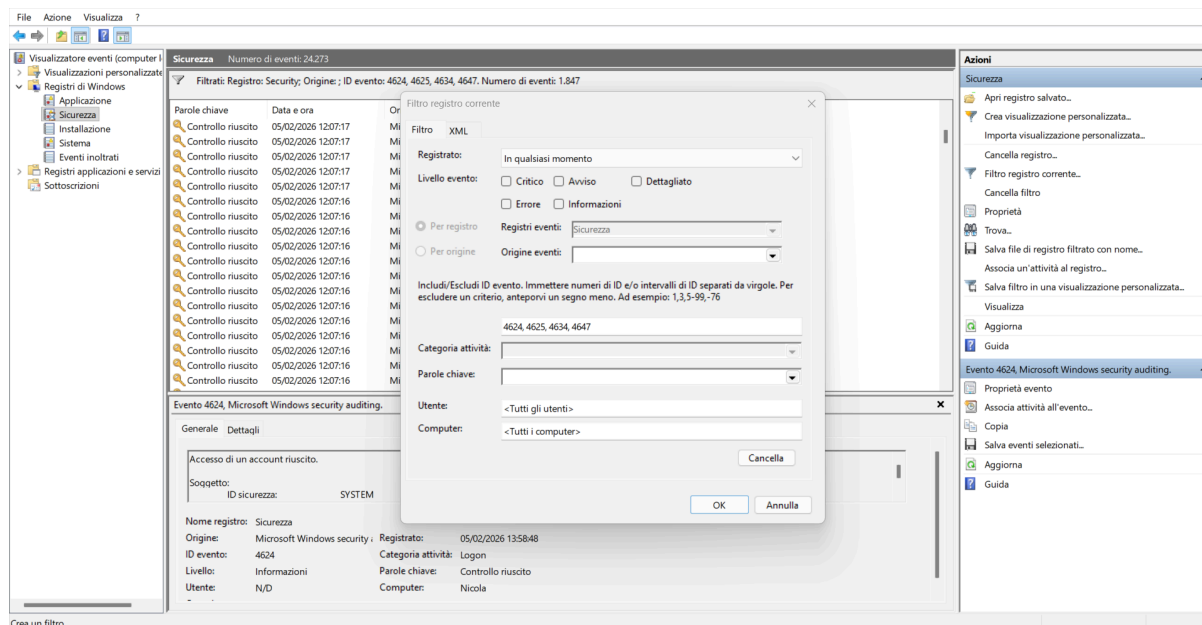


Figura 3: Applicazione della regola di filtraggio. Dettaglio della configurazione degli ID Evento target. Sono stati inseriti gli ID **4624** (Login riuscito), **4625** (Login fallito), **4634** e **4647** (Logoff) per isolare esclusivamente il ciclo di vita delle sessioni di autenticazione, escludendo le attività di sistema automatiche.

3.2 Decodifica degli ID Applicati

La scelta di questi specifici ID risponde a precise necessità di sicurezza:

1. **4624 (Logon):** Accesso riuscito. Fondamentale per stabilire la presenza di un utente.
2. **4625 (Logon Failure):** Accesso negato. È l'indicatore primario di tentativi di indovinare la password o attacchi dizionario.
3. **4634/4647 (Logoff):** Chiusura della sessione. Necessari per calcolare la durata della permanenza di un utente nel sistema.

4. Analisi dei Risultati Post-Filtro

L'applicazione del filtro ha prodotto un immediato miglioramento nella leggibilità e nell'utilità dei dati.

- **Riduzione del Rumore:** Il numero di eventi visibili è sceso da 24.281 a **1.848 eventi pertinenti**.
- **Visibilità Operativa:** La vista filtrata mostra ora una sequenza chiara di eventi **4624 (Logon)**, permettendo di ricostruire la timeline degli accessi.
- **Dettaglio Evento:** L'analisi di un singolo evento 4624 (evidenziato nel report) conferma l'avvenuto accesso con privilegi "SYSTEM" o utente, registrato con precisione al secondo (es. 14:00:10).

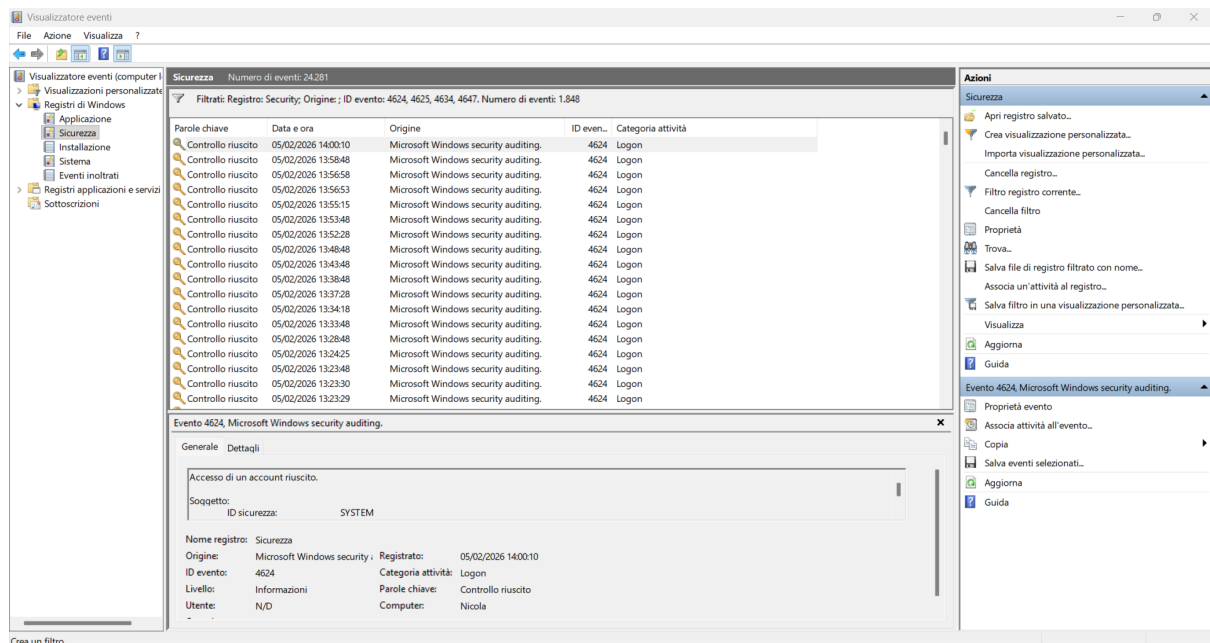


Figura 4: Esito dell'attività di Data Reduction. Il registro filtrato mostra ora un numero gestibile di eventi (riduzione da ~24.000 a ~1.800). La lista ripulita permette all'analista di visualizzare cronologicamente gli accessi riusciti (ID 4624) e verificare i dettagli dell'account nel pannello sottostante.

5. Conclusioni e Raccomandazioni

L'attività svolta dimostra come la corretta configurazione del Visualizzatore Eventi trasformi i log da semplici dati archiviati a strumenti di intelligence attiva.

Prossimi passi consigliati:

1. **Monitoraggio Attivo:** Controllare periodicamente la presenza dell'ID **4625**. Una sequenza rapida di questi eventi deve innescare un allarme immediato.
2. **Esportazione:** Salvare periodicamente le viste filtrate ("Salva file di registro filtrato con nome") per mantenere uno storico in caso di cancellazione accidentale o malevola dei log (Wiping).
3. **Correlazione:** In un ambiente aziendale, questi log dovrebbero essere inviati a un SIEM (Security Information and Event Management) per essere incrociati con dati di rete.