REPORT TECNICO

File di Log di Windows

Redatto da: *Nicolò Calì Cybersecurity Student*

Data: 05/02/2026

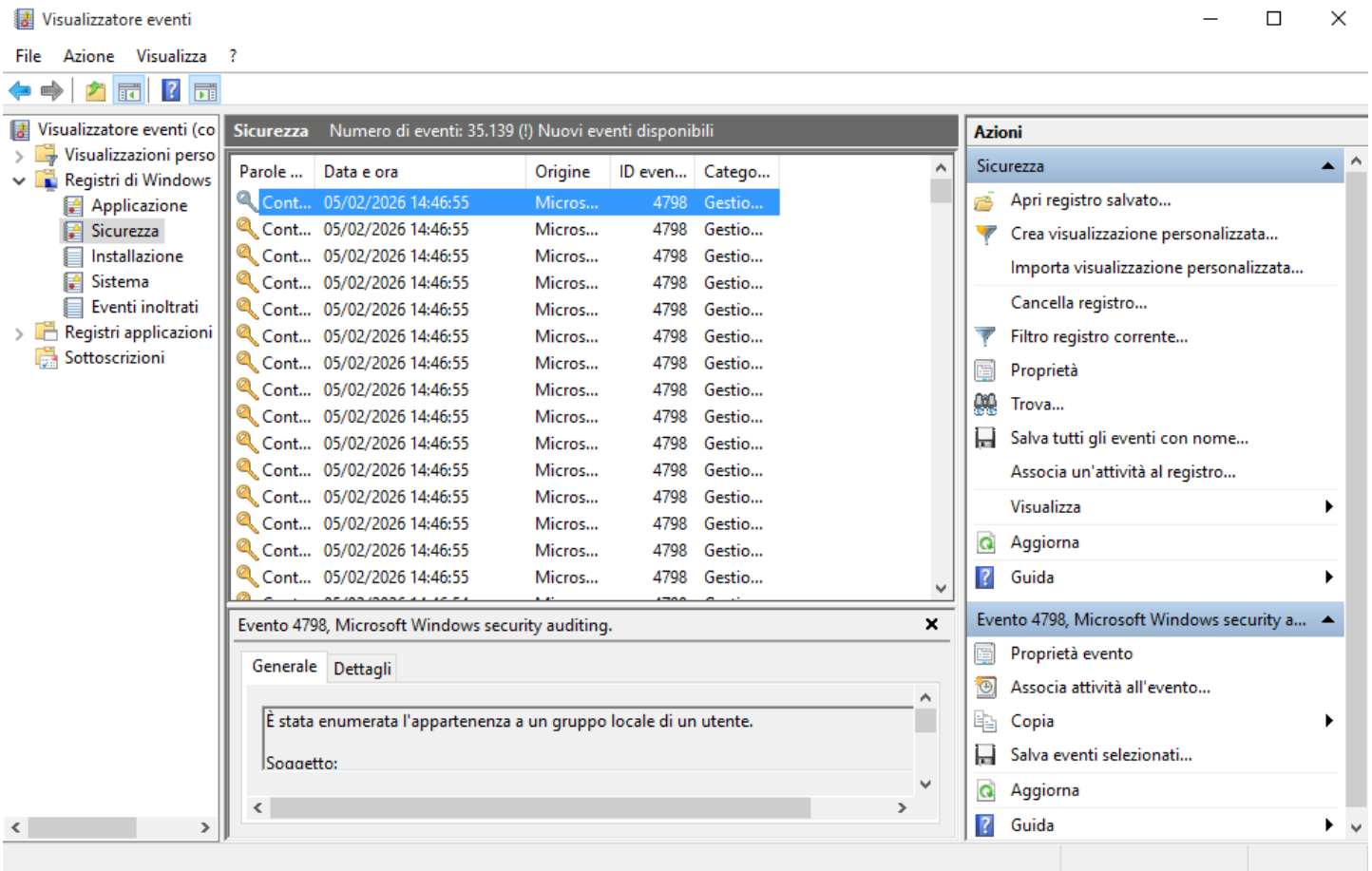
Oggetto: Implementazione di policy di auditing per il monitoraggio degli accessi

1. Introduzione

Il presente documento descrive le procedure di configurazione e analisi dei **log** di sicurezza in ambiente **Windows 10**. L'obiettivo dell'attività è abilitare il tracciamento degli eventi di accesso (*Logon/Logoff)* per monitorare sia le autenticazioni legittime che i tentativi di intrusione potenzialmente malevoli.

L'attività è stata svolta su una Macchina Virtuale Windows 10, utilizzando i seguenti strumenti nativi di amministrazione:

- **Criteri di sicurezza locali (secpol.msc):** Per la definizione delle regole di auditing.
- **Visualizzatore eventi (eventvwr):** Per la consultazione e l'analisi forense dei log generati.



2. Configurazione della Policy

Per abilitare la registrazione degli eventi, è necessario modificare i criteri di controllo locali. Senza questa configurazione, il sistema non conserverebbe traccia dei tentativi di accesso.

Procedura:

1. Accesso allo strumento di gestione tramite il comando **`secpol.msc`** eseguito con privilegi amministrativi.

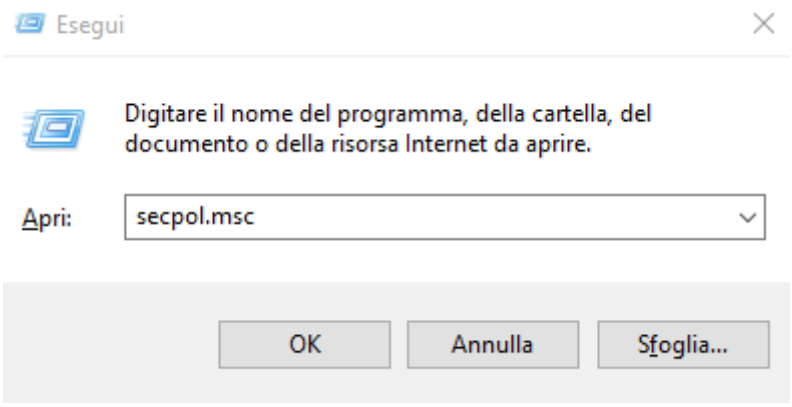


Fig. 1 Eseguire lo Strumento di Gestione delle Policy

2. Navigazione nel percorso: ***Criteri locali*** > ***Criteri controllo***.
3. Modifica della policy **"Controlla eventi di accesso"**.

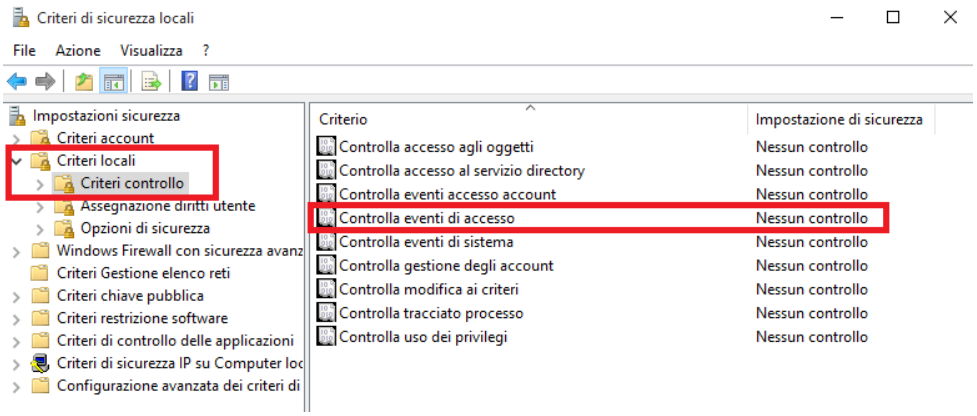


Fig. 2 Controllo eventi di accesso

Come mostrato nella figura sottostante, la policy è stata configurata per registrare sia gli eventi di **Successo** (utili per tracciare l'attività legittima degli utenti) che quelli di **Errore** (fondamentali per rilevare tentativi di accesso non autorizzato).

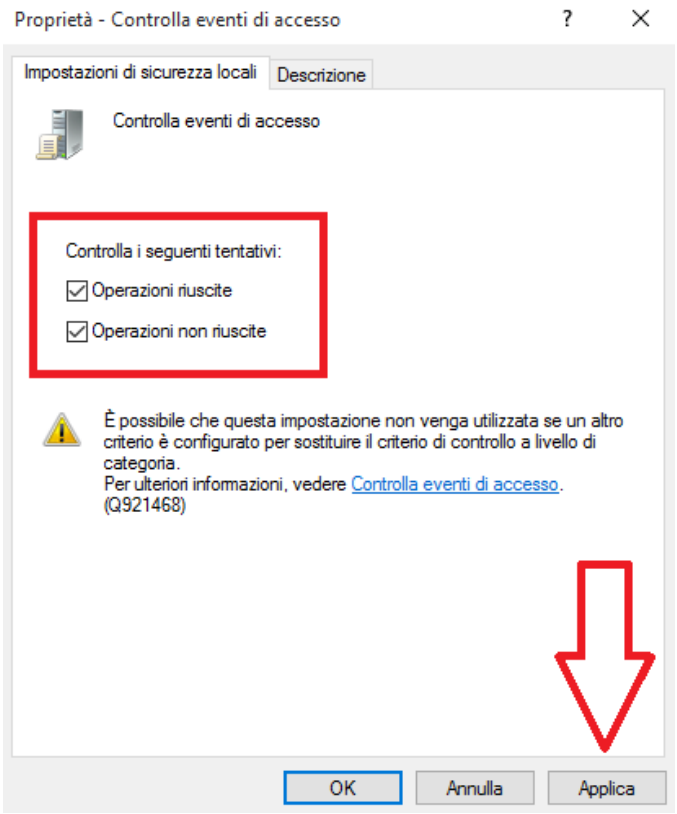


Fig. 3 Attivare policy di accesso

Assicuriamoci di cliccare su “**Applica**” per salvare le modifiche che sono state apportate alla Policy di Accesso.

3. Analisi degli Eventi

Una volta applicata la policy, è stata effettuata una simulazione per generare dati di log significativi:

1. Esecuzione di **due tentativi di accesso falliti** (inserimento volontario di password errata) per simulare un attacco *Brute Force* o un errore utente.
2. Esecuzione di un **accesso riuscito** con le credenziali corrette.

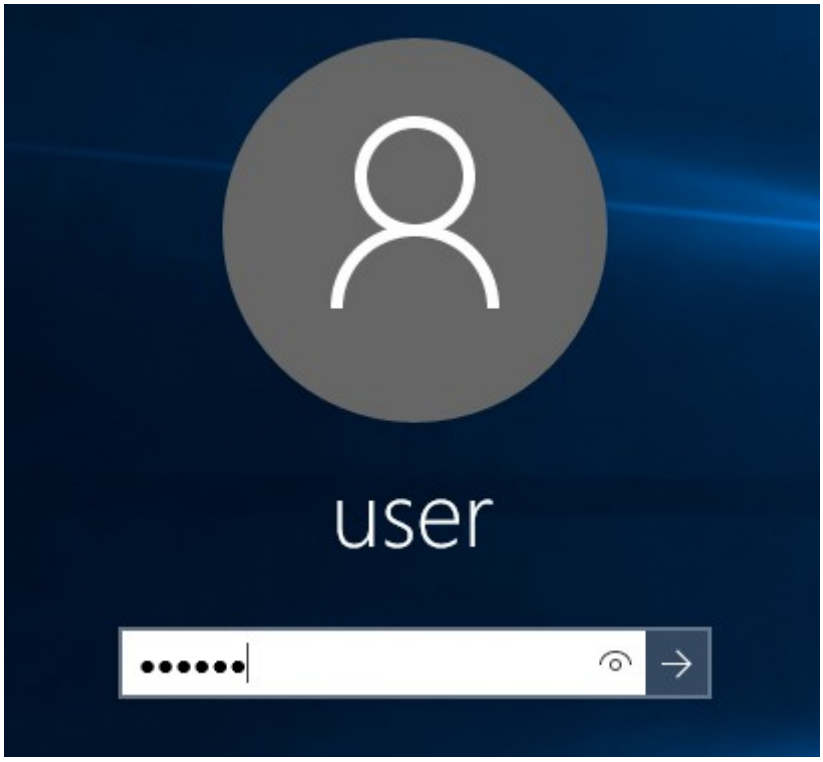


Fig. 4 Schermata di accesso Windows 10

Successivamente, si è proceduto all'analisi tramite il **Visualizzatore Eventi**.

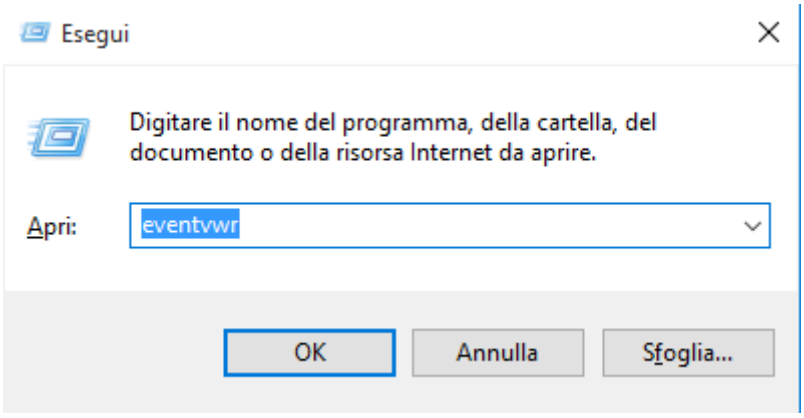


Fig. 5 Eseguire lo Strumento di Gestione eventi

3.1 Filtraggio dei Log

Data l'elevata mole di dati presenti nel registro "Sicurezza", è stato applicato un filtro mirato per isolare solo gli eventi di interesse, utilizzando gli ID evento specifici per le operazioni di login:

- ID 4624: Accesso riuscito.
- ID 4625: Accesso non riuscito.

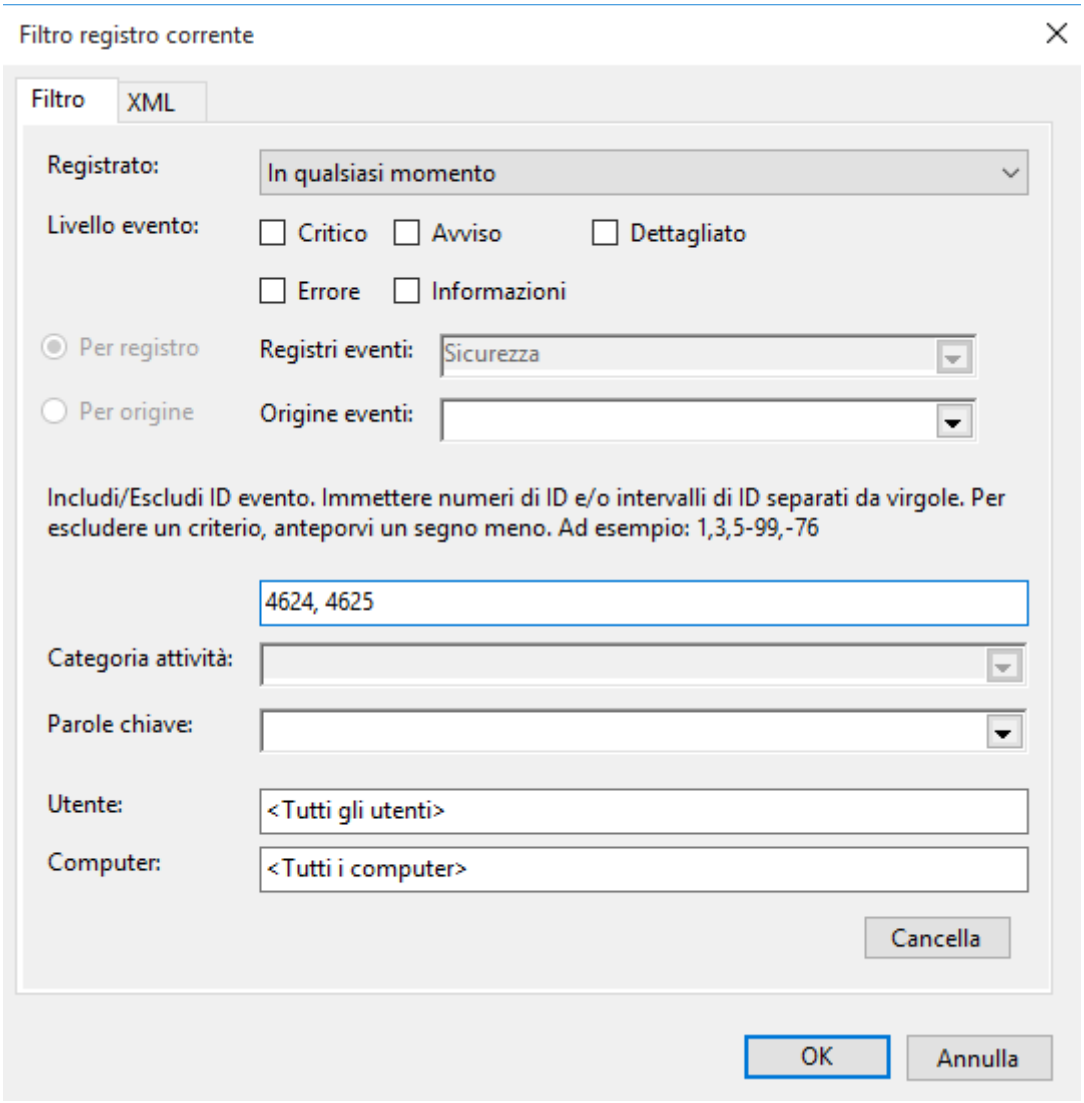


Fig. 6 Opzioni di Filtraggio dei Log

3.2 Risultati del monitoraggio

Il filtraggio ha restituito una cronologia chiara degli **eventi**, evidenziando la sequenza temporale delle azioni. Nella lista seguente è possibile distinguere visivamente i **tentativi falliti** (*contrassegnati dall'icona del lucchetto chiuso*) dagli **accessi riusciti** (*icona chiave/lucchetto aperto*).

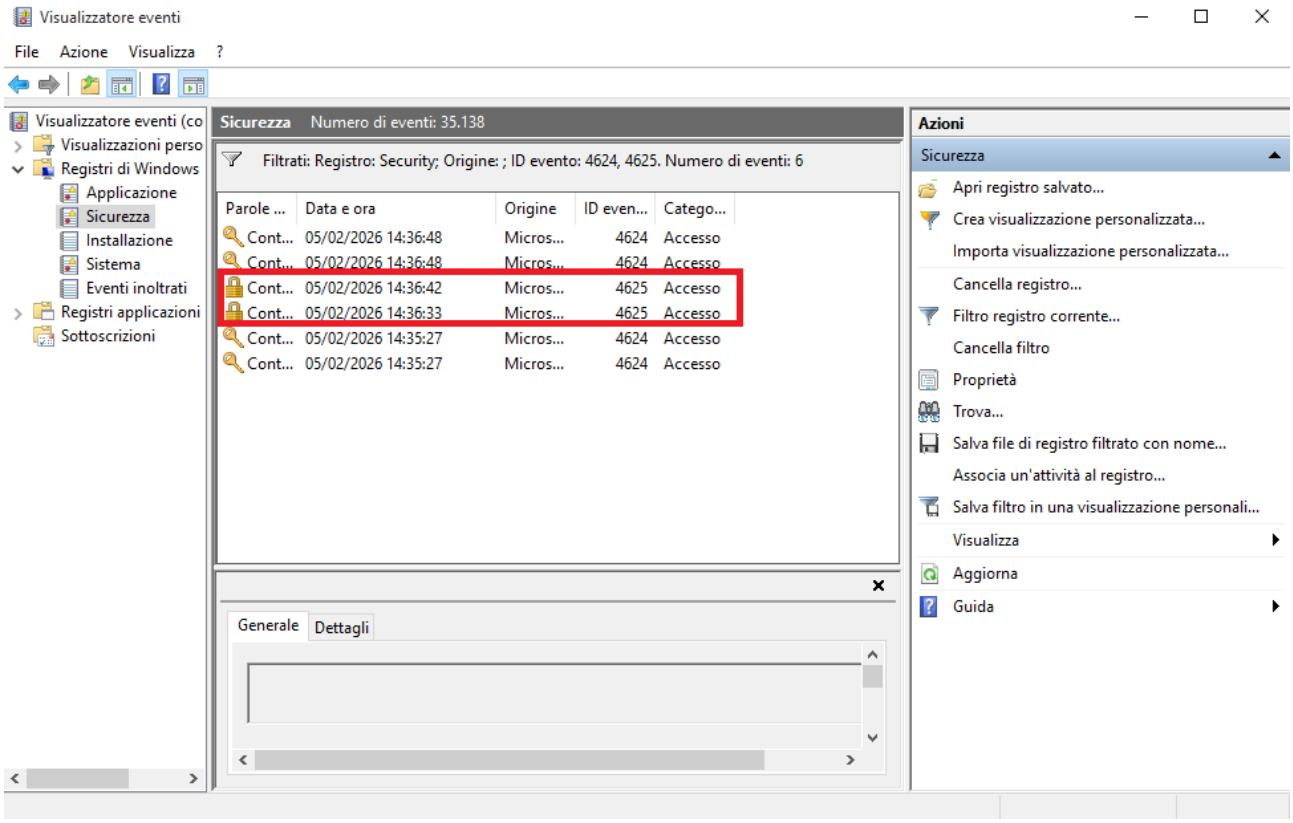


Fig. 7 Eventi di accesso

3.3 Analisi dettagliata

Analizzando il dettaglio di uno degli eventi di errore (**ID 4625**), siamo in grado di estrarre informazioni cruciali per un'indagine forense.

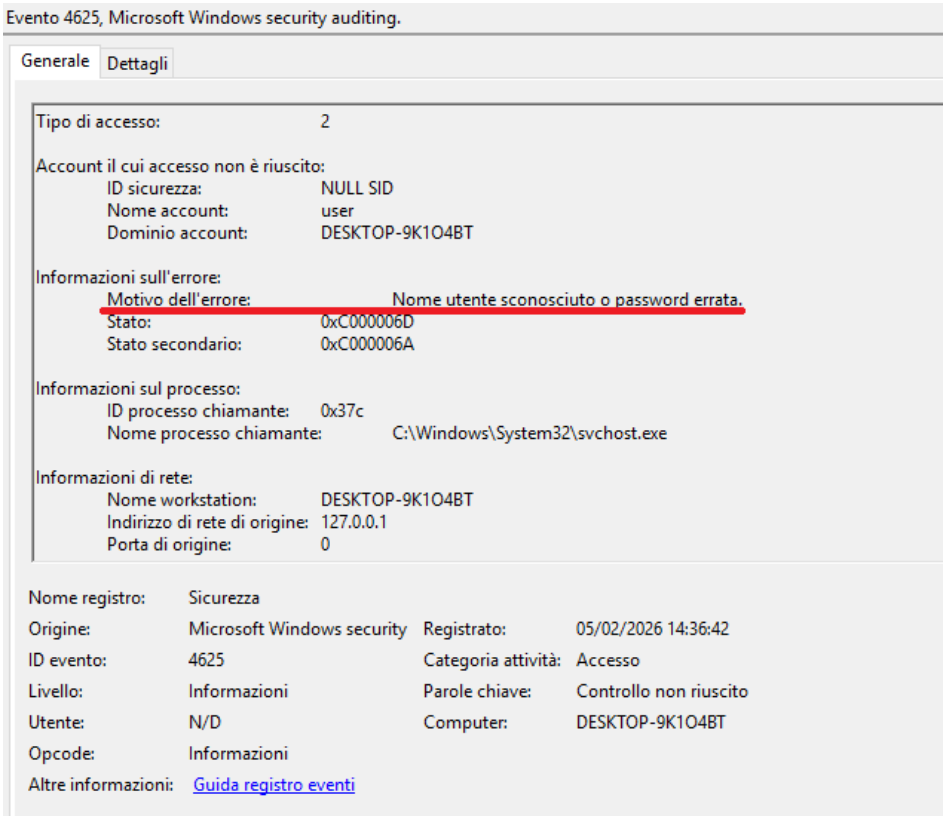


Fig. 8 Informazioni relative all'accesso

Dall'analisi dell'immagine sopra riportata emergono i seguenti dati:

- **Account coinvolto:** `user` (l'account target del tentativo).
- **Motivo dell'errore:** "Nome utente sconosciuto o password errata".
- **Origine:** L'indirizzo di rete `127.0.0.1` indica che il tentativo è avvenuto localmente sulla macchina stessa (`DESKTOP-9K104BT`), e non da remoto.
- **Processo chiamante:** `svchost.exe` (processo di sistema relativo al login screen).

6. Conclusione e Considerazioni

L'attività ha dimostrato l'importanza fondamentale dei log di Windows per la sicurezza informatica. La corretta configurazione delle **Audit Policy** permette di trasformare un sistema passivo in uno strumento di monitoraggio attivo.

Per un **SOC Analyst**, la capacità di leggere e interpretare eventi come il **4625** è critica.

Un singolo evento 4625 può essere un semplice errore di digitazione, ma una sequenza rapida e ripetuta di questi eventi è un forte indicatore di compromissione per attacchi di tipo **Password Guessing** o **Brute Force**.

Saper filtrare e analizzare questi dati permette di ridurre il "rumore" di fondo e concentrarsi sulle reali minacce alla sicurezza dell'infrastruttura.