File di Log di Windows

06/02/2025

TRACCIA

Configurare e gestire i file di log della sicurezza utilizzando il Visualizzatore eventi di Windows.

Istruzioni:

1. Accedere al Visualizzatore Eventi:

- Apri il Visualizzatore eventi premendo Win + R per aprire la finestra "Esegui".
- Digita eventvwr e premi Invio.

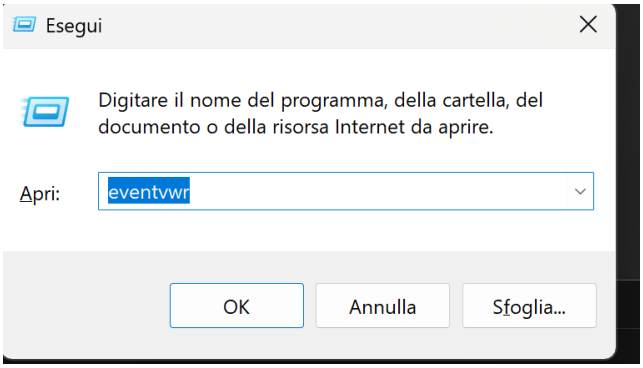
2. Configurare le Proprietà del Registro di Sicurezza:

- Nel pannello di sinistra, espandi "Registri di Windows" e seleziona "Sicurezza".

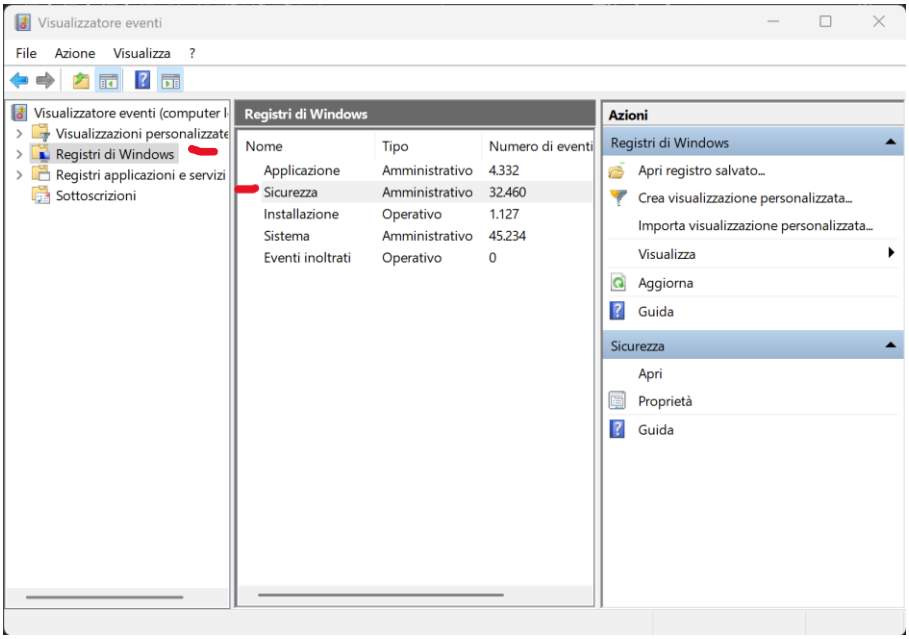
3. Analizzare gli eventi con Categoria Attività Logon e Special Logon

SVOLGIMENTO

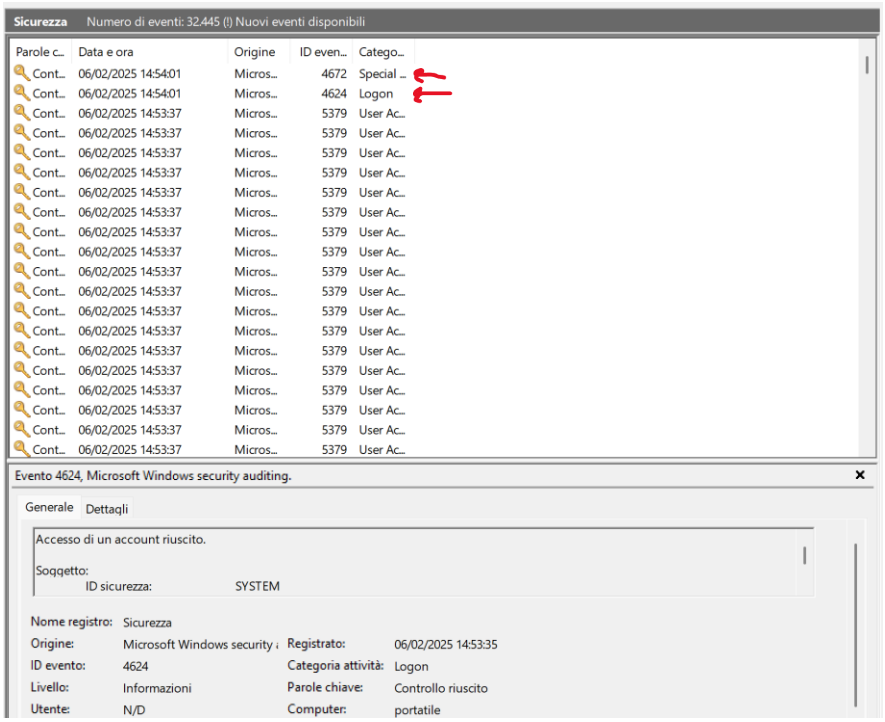
Apro la finestra “esegui” e digito “eventvwr” per entrare nel visualizzatore eventi:



Entrato dentro mi sposto nel pannello a sinistra ed espando “registri windows” e entro dentro “sicurezza”:



Come richiesto dalla traccia andremo ad analizzare gli eventi con categoria Accesso (Logon) e Accesso Speciale (Special Logon):



Logon:

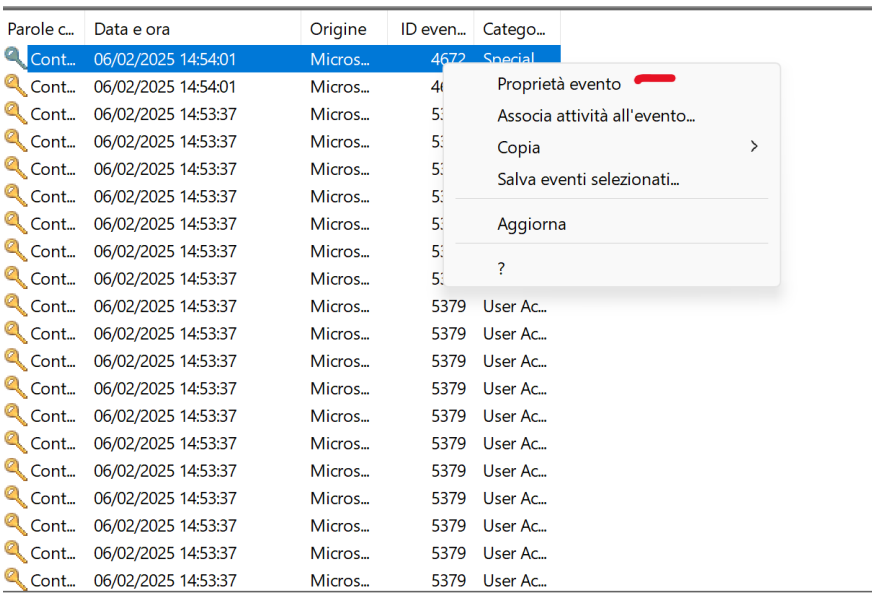
- Si verifica ogni volta che un utente si autentica a un sistema o a un'applicazione.
- Gli eventi di logon includono l'accesso a computer, server, reti e altre risorse digitali.
- Questi eventi sono tracciati per scopi di sicurezza, permettendo di monitorare chi ha accesso a cosa e quando.

Special Logon:

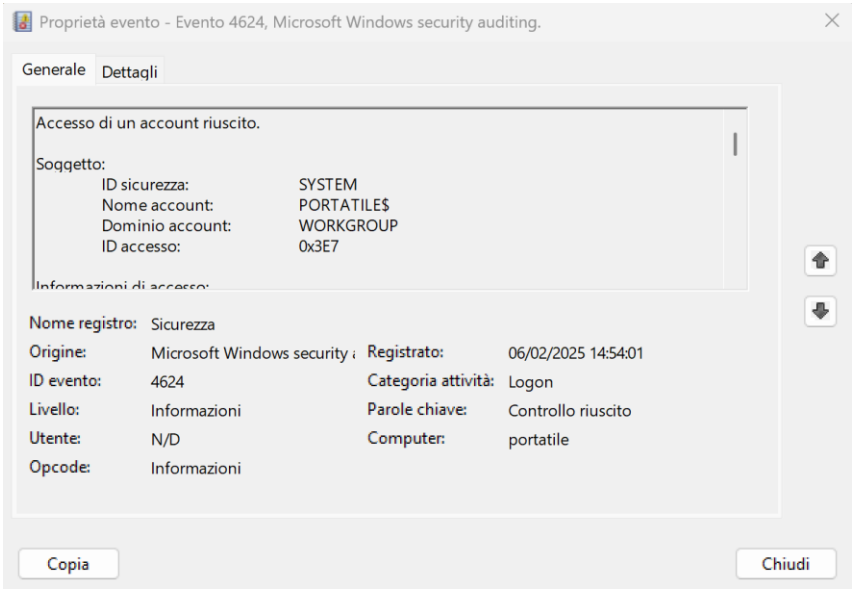
- Si riferisce a un accesso con credenziali elevate o privilegi amministrativi.
- Questi accessi sono particolarmente importanti perché gli utenti con permessi elevati hanno accesso a funzionalità sensibili e critiche del sistema.

- Gli eventi di special logon aiutano a garantire che solo il personale autorizzato stia utilizzando i privilegi elevati, contribuendo a prevenire abusi o attacchi interni.

Per analizzare più precisamente gli eventi basterà cliccare su un evento, premere il tasto destro e cliccare su “proprietà evento” per avere maggiori dettagli:



Una volta che gli diamo il comando ci apparirà una schermata di questo tipo:



Nella parte finale della sezione “Generale” troviamo anche una spiegazione dell’evento.

Questo evento viene generato quando viene creata una sessione di accesso. Viene generato nel computer in cui è stato effettuato l'accesso.

Il campo Soggetto indica l'account nel sistema locale che ha richiesto l'accesso. Generalmente si tratta di un servizio, quale il servizio Server, o di un processo locale, ad esempio Winlogon.exe o Services.exe.

Il campo Tipo di accesso indica il tipo di accesso che È stato effettuato. I tipi più comuni sono 2

Cosa analizzare e perchè

Eventi di Accesso= (Logon - 4624)

Cosa analizzare:

- Account utilizzato per l'accesso.
- Indirizzo IP (se remoto).
- Tipo di accesso (ad es. interattivo, remoto, rete).

Perché:

- Per verificare quali utenti accedono al sistema.
- Per identificare accessi sospetti o non autorizzati.

Informazioni di accesso:

Tipo di accesso:	5
Modalità amministrativa limitata::	-
Credential Guard remoto:	-
Account virtuale:	No
Token elevato:	Sì

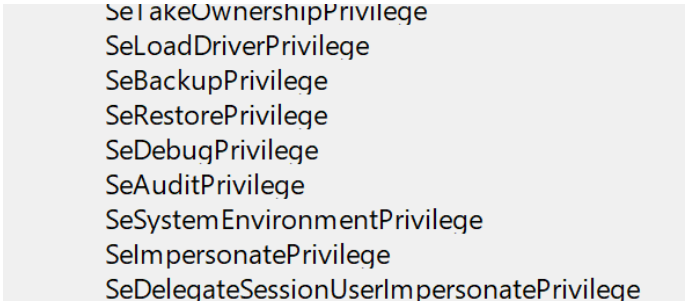
Nuovo accesso:

ID sicurezza:	SYSTEM
Nome account:	SYSTEM
Dominio account:	NT AUTHORITY
ID accesso:	0x3E7
ID accesso collegato:	0x0
Nome account di rete:	-
Dominio account di rete:	-
GUID accesso:	{00000000-0000-0000-0000-000000000000}

nformazioni sul processo:

ID processo:	0x5f0
Nome processo:	C:\Windows\System32\services.exe

Ora analizziamo uno special logon:



Accesso Speciale (Special Logon - 4672)

Cosa analizzare:

- Account che ha eseguito l'accesso speciale.
- Privilegi assegnati all'utente.
- Ora e data dell'evento.

Perché:

- Indica l'uso di account amministrativi o privilegiati. Utile per monitorare attività sospette di utenti con privilegi elevati.