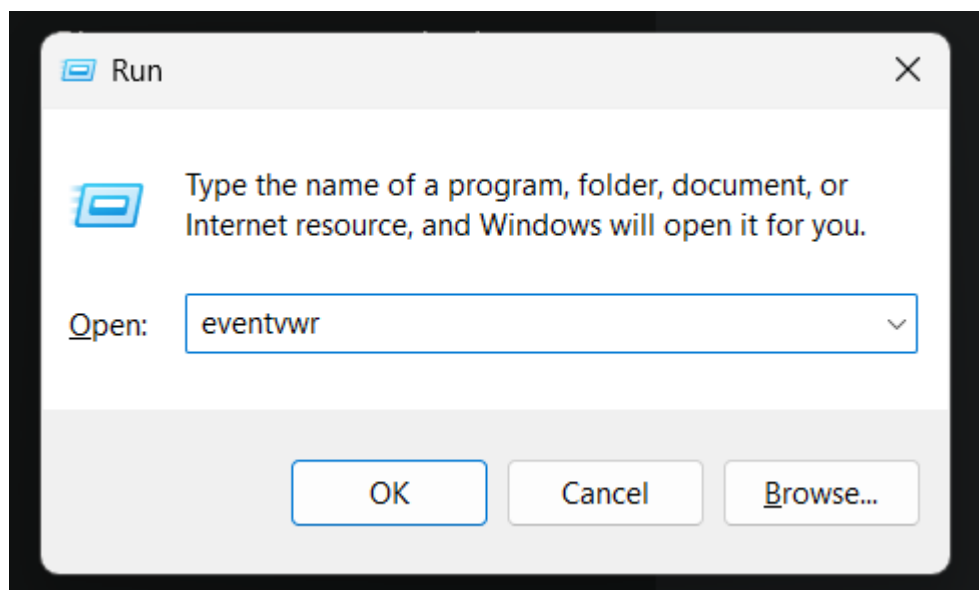


S9L4

Esercizio di oggi: Creazione e Gestione delle Regole per i File di Log della Sicurezza in Windows

Apri la finestra "Esegui":

Premi i tasti **Win + R**.



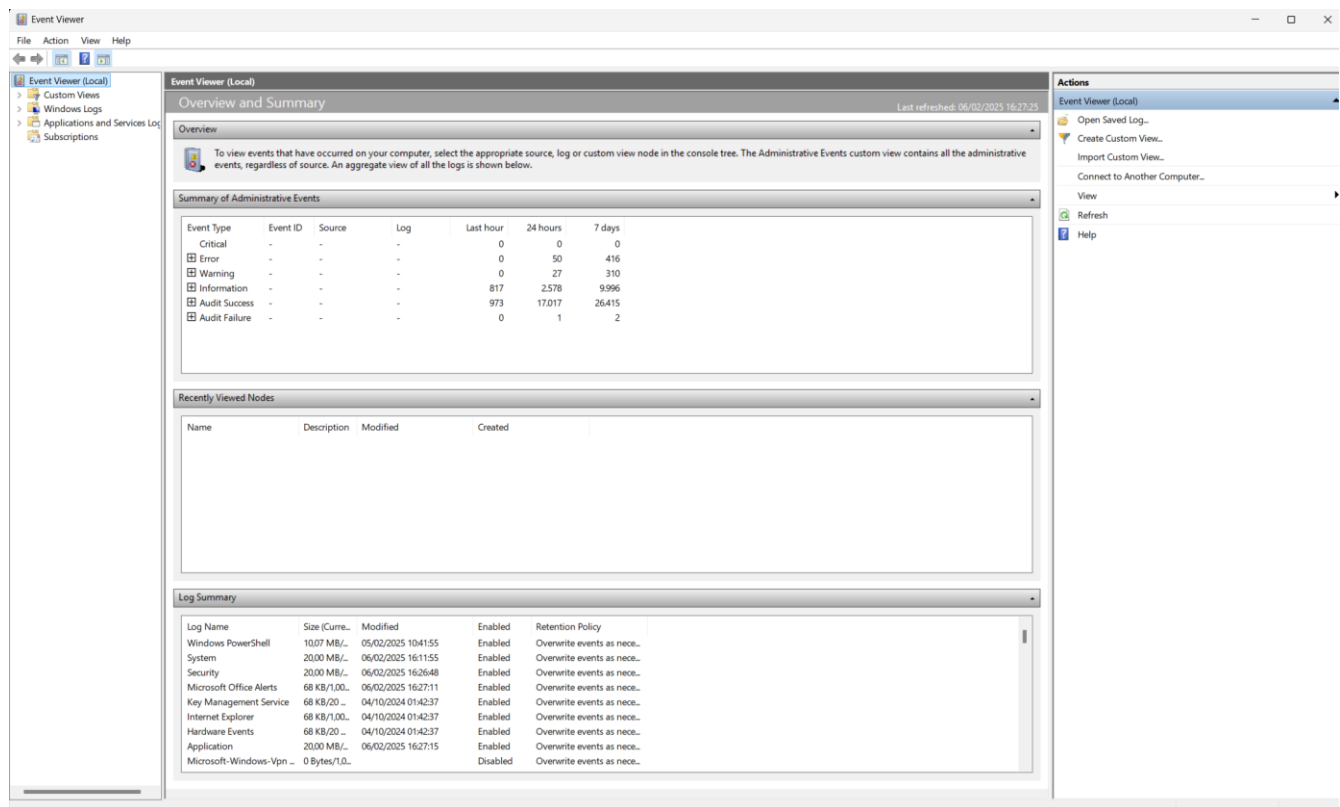
Avvia il Visualizzatore eventi:

"Esegui" digita **eventvwr** e premi **Invio**.

Questo comando aprirà il Visualizzatore eventi, lo strumento di Windows che consente di visualizzare i vari log di sistema.

Espando la sezione "Registri di Windows":

Nel pannello di sinistra del Visualizzatore eventi, c'è una struttura ad albero. Sulla freccia accanto a **Registri di Windows** per espandere la sezione.



Seleziona il Registro "Sicurezza":

Sicurezza


In questo registro sono memorizzati gli eventi relativi alla sicurezza del sistema, come tentativi di accesso (logon) e altre attività che riguardano la gestione degli accessi.


editing.
editing.
editing.
editing.
editing.
editing.
editing.
editing.
editing.
editing.
editing.

×

Actions


Security ▲

 Open Saved Log...


 Create Custom View...


Import Custom View...


Clear Log...

 Filter Current Log...


Clear Filter

 Properties


 Find...


 Save Filtered Log File As...

Attach a Task To this Log...


 Save Filter to Custom View...


View ►


 Refresh


 Help

Event 4672, Microsoft Windows security auditing. ▲


 Event Properties

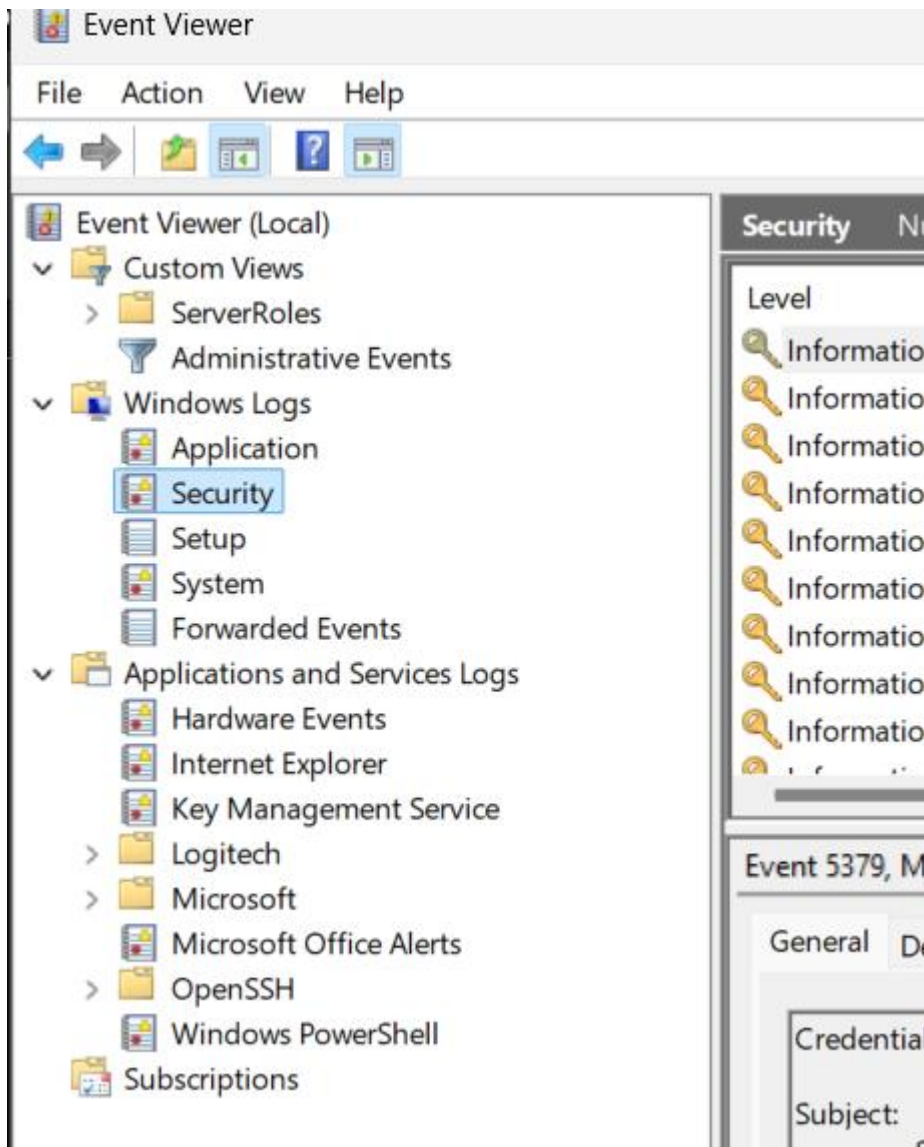
 Attach Task To This Event...

 Save Selected Events...

 Copy

 ►

 Refresh



Filter Current Log



Filter

XML

Logged:

Any time



Event level:

☐

Critical

☐

Warning

☐

Verbose

☐

Error

☐

Information

☒ By log

Event logs:

Security

☐ By source

Event sources:



Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4626,4625,4672

Task category:



Keywords:



User:

<All Users>

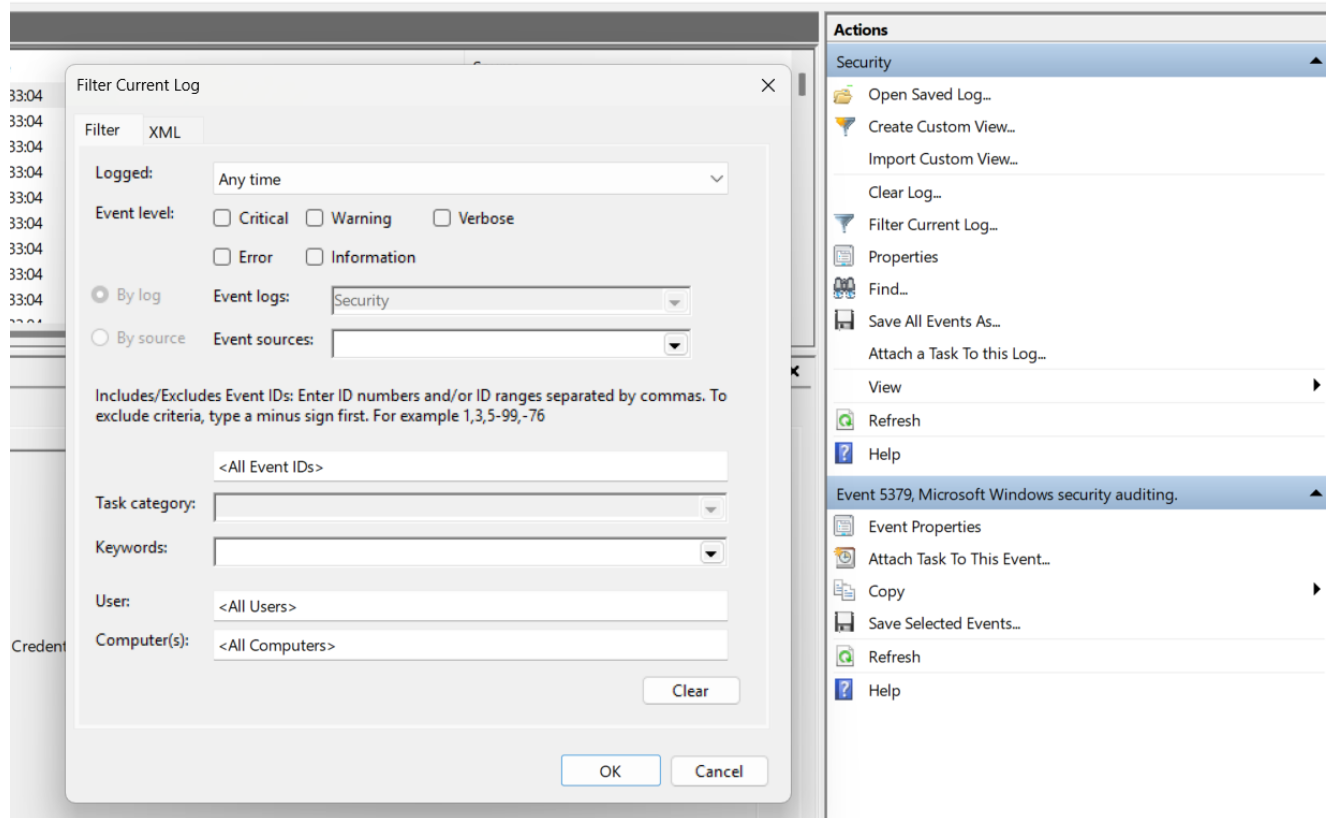
Computer(s):

<All Computers>

Clear

OK

Cancel



Gli **eventi di Logon** solitamente includono l'ID **4624** (accesso riuscito) e **4625** (accesso fallito) nelle versioni moderne di Windows.

Filter Current Log



Filter

XML

Logged: Any time ▼

Event level: ☐ Critical ☐ Warning ☐ Verbose☐ Error ☐ Information☒ By log

Event logs: Security ▼

☐ By source

Event sources: ▼

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4625

Task category:

▼

Keywords:

▼

User:

<All Users>

Computer(s):

<All Computers>

Clear

OK

Cancel

Security Number of events: 26397

Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 2

Level	Date and Time	Source
Information	06/02/2025 14:51:03	Microsoft Windows security auditing.
Information	04/02/2025 21:24:18	Microsoft Windows security auditing.

Event 4625, Microsoft Windows security auditing.

General Details

An account failed to log on.

Subject:

Security ID: SYSTEM
Account Name: [REDACTED]
Account Domain: WORKGROUP
Logon ID: 0x3E7

Logon Type: 2

Account For Which Logon Failed:

Security ID: NULL SID
Account Name: [REDACTED]
Account Domain: [REDACTED]

Failure Information:

Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A

Process Information:

Caller Process ID: 0xd3c
Caller Process Name: C:\Windows\System32\svchost.exe

Network Information:

Workstation Name: FISSO
Source Network Address: 127.0.0.1
Source Port: 0

Detailed Authentication Information:

Logon Process: User32
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

Log Name: Security
Source: Microsoft Windows security : Logged: 06/02/2025 14:51:03
Event ID: 4625 Task Category: Logon
Level: Information Keywords: Audit Failure
User: N/A Computer: [REDACTED]
OpCode: Info

This event is generated when a logon request fails. It is generated on the computer where access was attempted.

The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network).

The Process Information fields indicate which account and process on the system requested the logon.

The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The authentication information fields provide detailed information about this specific logon request.

- Transited services indicate which intermediate services have participated in this logon request.
- Package name indicates which sub-protocol was used among the NTLM protocols.
- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

Elementi interessanti:

Categoria attività: Dove vengono indicate le tipologie (ad esempio, "Logon" o "Special Logon").

Data e ora, ID utente, tipo di accesso, etc.

Queste informazioni ti permettono di comprendere meglio il comportamento del sistema in termini di sicurezza e accessi. In particolare, posso vedere un tentativo di login.

Filter Current Log

×

Filter

XML

Logged:

Any time

▼

Event level:

☐ Critical

☐ Warning

☐ Verbose

☐ Error

☐ Information

☒ By log

Event logs:

Security

▼

☐ By source

Event sources:

▼

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

4626

Task category:

▼

Keywords:

▼

User:

<All Users>

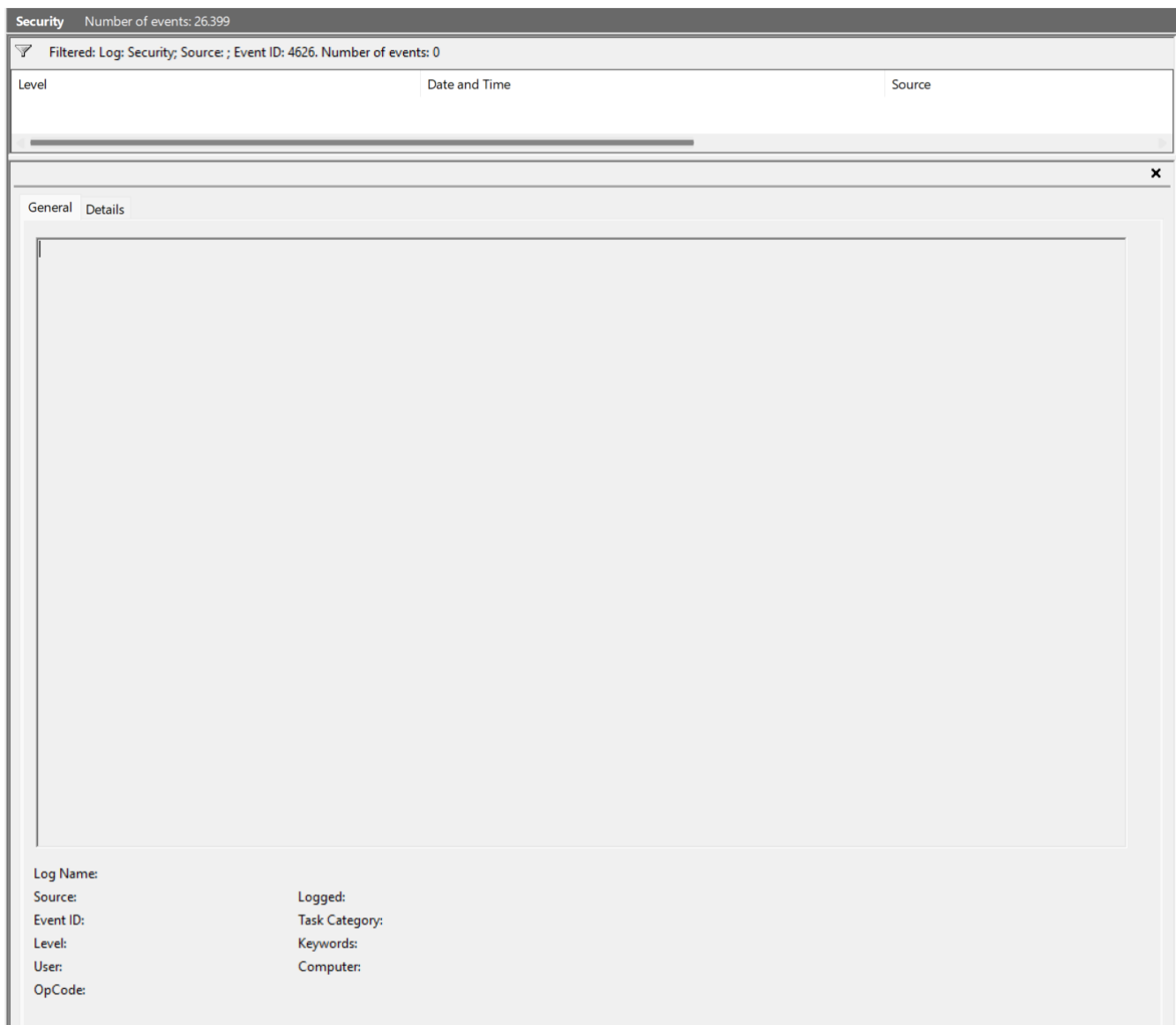
Computer(s):

<All Computers>

Clear

OK

Cancel



Gli **eventi di Special Logon** possono essere associati a particolari privilegi elevati. Ad esempio, l'evento **4672** segnala l'assegnazione di privilegi speciali al momento del logon

Security Number of events: 26399

Filtered: Log: Security; Source: ; Event ID: 4672. Number of events: 969

Level	Date and Time	Source
Information	06/02/2025 16:39:29	Microsoft Windows security auditing.
Information	06/02/2025 16:38:33	Microsoft Windows security auditing.
Information	06/02/2025 16:33:04	Microsoft Windows security auditing.
Information	06/02/2025 16:26:11	Microsoft Windows security auditing.
Information	06/02/2025 16:24:23	Microsoft Windows security auditing.
Information	06/02/2025 16:05:41	Microsoft Windows security auditing.
Information	06/02/2025 16:05:39	Microsoft Windows security auditing.
Information	06/02/2025 16:05:38	Microsoft Windows security auditing.
Information	06/02/2025 16:05:38	Microsoft Windows security auditing.
Information	06/02/2025 16:05:37	Microsoft Windows security auditing.
Information	06/02/2025 16:05:36	Microsoft Windows security auditing.
Information	06/02/2025 16:05:36	Microsoft Windows security auditing.
Information	06/02/2025 16:05:36	Microsoft Windows security auditing.

Event 4672, Microsoft Windows security auditing.

General Details


Special privileges assigned to new logon.

Subject:

Security ID: SYSTEM
Account Name: SYSTEM
Account Domain: NT AUTHORITY
Logon ID: 0x3E7

Privileges:

SeAssignPrimaryTokenPrivilege
SeTcbPrivilege
SeSecurityPrivilege
SeTakeOwnershipPrivilege
SeLoadDriverPrivilege
SeBackupPrivilege
SeRestorePrivilege
SeDebugPrivilege
SeAuditPrivilege
SeSystemEnvironmentPrivilege
SeImpersonatePrivilege
SeDelegateSessionUserImpersonatePrivilege

Log Name: Security
Source: Microsoft Windows security : Logged: 06/02/2025 16:39:29
Event ID: 4672 Task Category: Special Logon
Level: Information Keywords: Audit Success
User: N/A Computer: 
OpCode: Info

L'evento **4672 (Special Logon)** indica che un account ha ricevuto privilegi elevati al momento dell'accesso.

Dati chiave dell'evento:

- **Account:** SYSTEM (NT AUTHORITY)
- **Privilegi assegnati:** Permessi critici come SeDebugPrivilege, SeLoadDriverPrivilege, SeTakeOwnershipPrivilege, ecc.
- **Origine:** Windows Security Audit
- **Data/Ora:** 06/02/2025 - 16:39:29
- **Computer:** HIDDEN

Interpretazione:

Questo evento segnala che l'account SYSTEM ha ottenuto privilegi amministrativi avanzati. È normale per processi di sistema, ma se appare per un account utente potrebbe indicare un potenziale rischio di sicurezza.

Ecco un riepilogo dei privilegi assegnati nell'**evento 4672 (Special Logon)**:

1. **SeAssignPrimaryTokenPrivilege** – Permette di sostituire il token di accesso di un processo, utile per l'impersonificazione di utenti.
2. **SeTcbPrivilege** – Indica che il processo fa parte del sistema operativo ed è attendibile per gestire credenziali di sicurezza (Trusted Computing Base).
3. **SeSecurityPrivilege** – Consente la gestione di audit e log di sicurezza, incluso l'accesso ai registri degli eventi di sicurezza.
4. **SeTakeOwnershipPrivilege** – Permette di assumere la proprietà di file e oggetti senza il permesso esplicito del proprietario.
5. **SeLoadDriverPrivilege** – Autorizza il caricamento e la gestione di driver di sistema, con potenziali impatti sulla sicurezza.
6. **SeBackupPrivilege** – Consente di eseguire operazioni di backup ignorando i permessi standard sui file.
7. **SeRestorePrivilege** – Permette il ripristino di file ignorando le autorizzazioni, utile nelle operazioni di recovery.
8. **SeDebugPrivilege** – Permette di eseguire il debug su qualsiasi processo, inclusi quelli di sistema e altri utenti, un rischio se sfruttato da malware.
9. **SeAuditPrivilege** – Consente la configurazione e la gestione delle policy di audit di sicurezza del sistema.
10. **SeSystemEnvironmentPrivilege** – Permette la modifica delle variabili di sistema a basso livello.
11. **SeImpersonatePrivilege** – Consente a un processo di assumere l'identità di un altro utente, utile per servizi e applicazioni con funzioni avanzate.
12. **SeDelegateSessionUserImpersonatePrivilege** – Permette l'impersonificazione di utenti in sessioni remote, aumentando i potenziali rischi se usato impropriamente.

Implicazioni di sicurezza

Questi privilegi sono altamente sensibili e normalmente assegnati solo ad account di sistema e amministratori. Potrebbe essere un segnale di **attività sospetta** o **compromissione** del sistema.