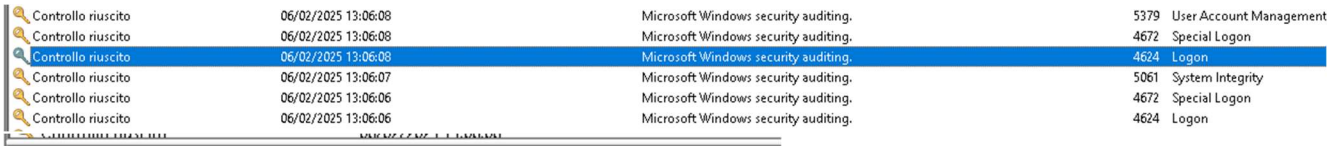
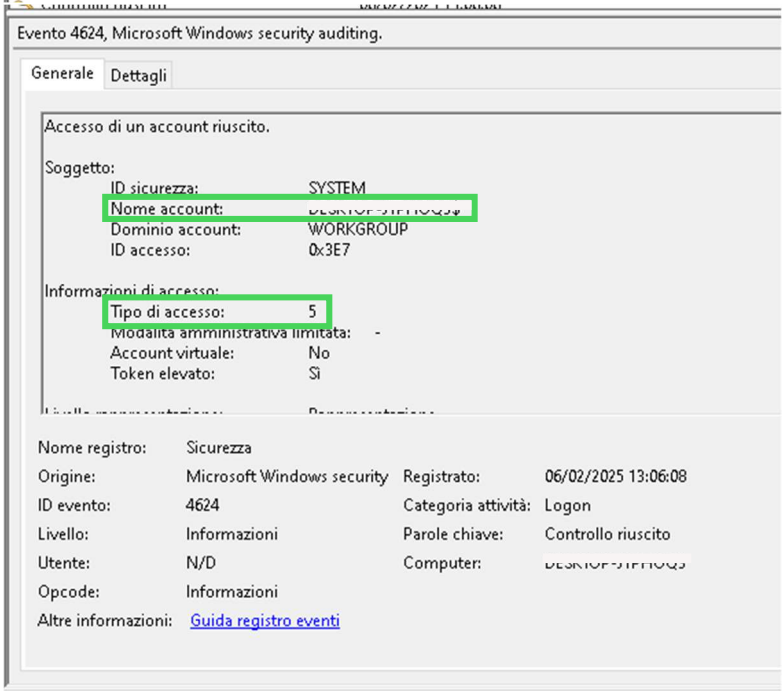
Gli eventi con categoria attività "Logon" e "Special Logon" sono fondamentali per monitorare l'accesso e la gestione delle credenziali nel sistema.
Questi eventi vengono registrati quando un utente tenta di accedere a un sistema Windows, indipendentemente dal successo o dal fallimento. I più rilevanti sono:

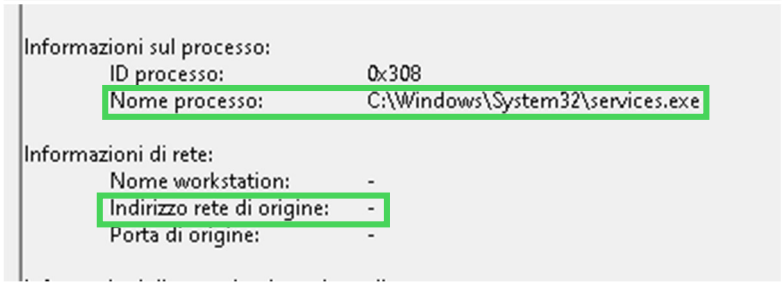
Event ID	Descrizione
4624	Accesso riuscito
4625	Tentativo di accesso fallito
4648	Accesso con credenziali esplicite
4672	Accesso con privileggi elevati

ID 4624

Significa che un utente o servizio è riuscito ad autenticarsi. Nei dettagli vengono specificati:
Account name: Nome utente autenticato
Logon Type: Determina il tipo di accesso in base a un numero (tabella sotto)
Source Network Address: indica l'indirizzo IP di origine
Process Name: indica il processo che ha gestito il logon

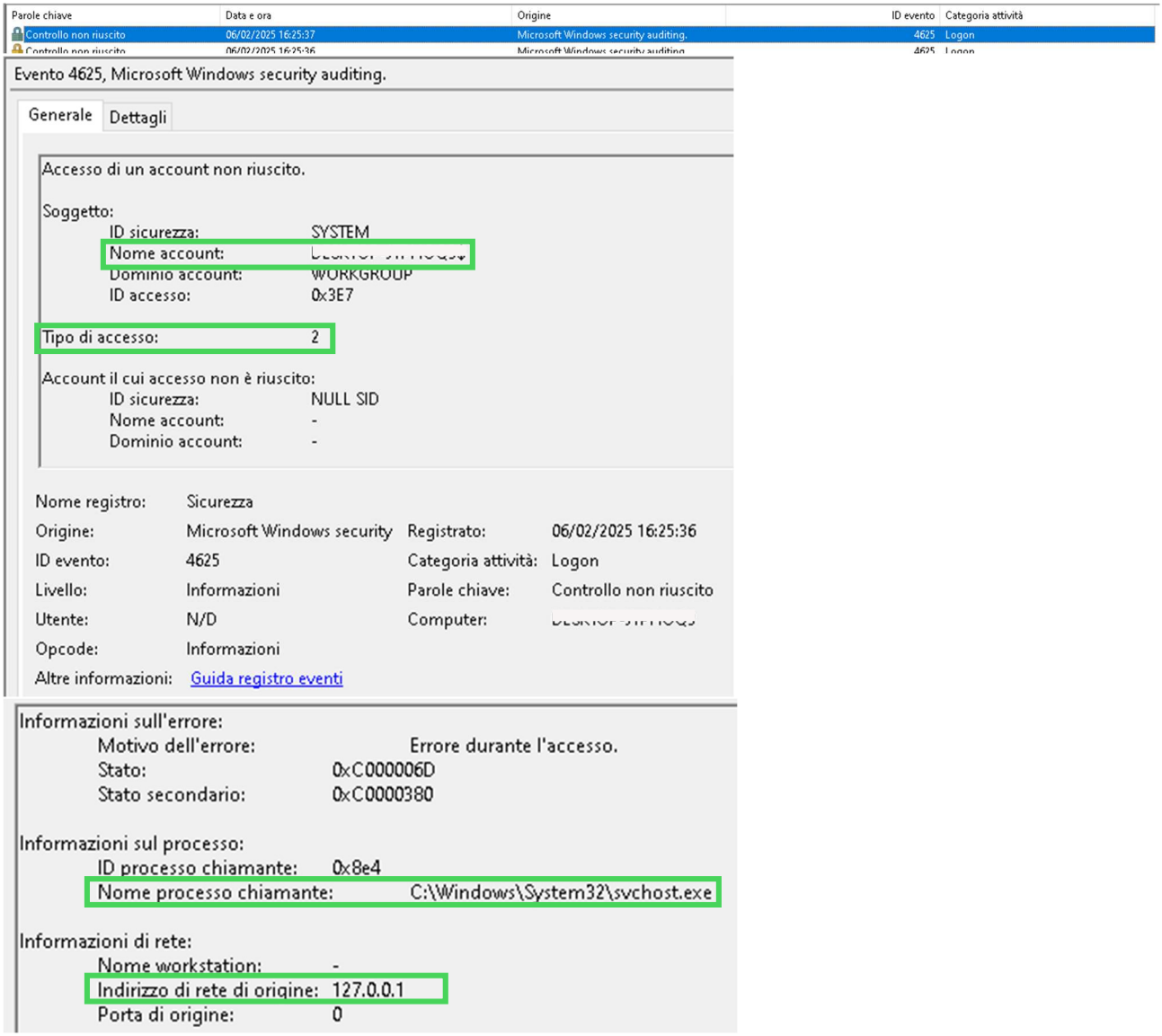






ID 4625

Indica un tentativo di accesso non riuscito. Questo codice è molto importante per individuare possibili attacchi di brute force o accessi non autorizzati. Nei dettagli vengono specificati:
Failure Reason: motivo del fallimento
Source network Address: IP sorgente del tentativo di autenticazione
Account For Witch Logon Failed: Nome utente bersagliato.
Per poter visualizzare questo processo, ho effettuato un logout dall'utente corrente premendo i tasti Win+L e messo delle credenziali errate.

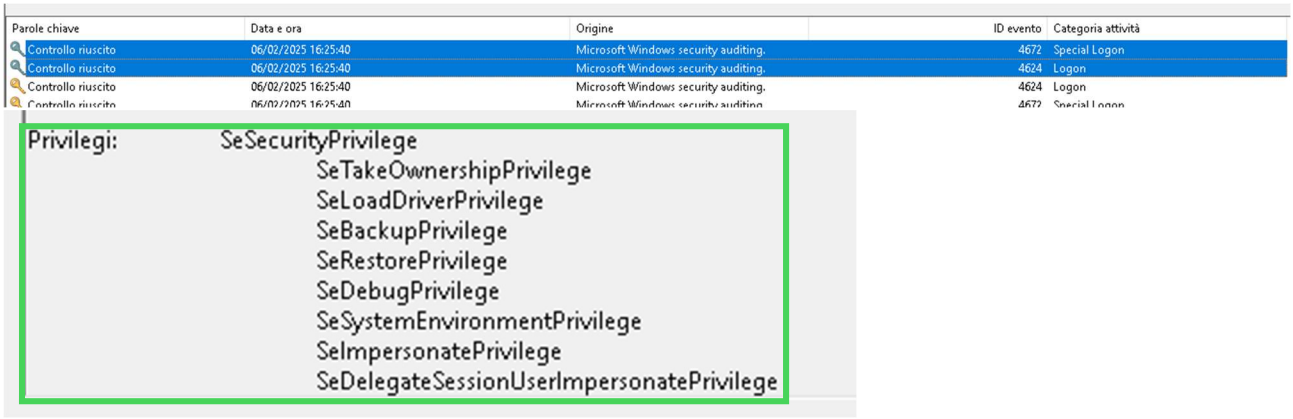


Il campo di **Logon Type** negli eventi di logon indica come è avvenuto l 'accesso:

Logon Type	Descrizione	Esempi D'uso
2	Interactive	Login con tastiera/mouse
3	Network	Accesso da rete
4	Batch	Script o processi automatizzati
5	Service	Account di servizio Windows
7	Unlock	Riattivazione da blocco schermo
8	NetworkClearText	Login via rete senza crittografia (!)
9	NewCredentials	Credenziali usate da un altro contesto
10	RemoteInteractive	Accesso da desktop remoto
11	CachedInteractive	Login con credenziali memorizzate (offline)

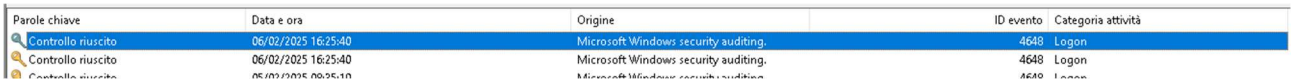
ID 4672

Il special logon viene registrato quando un utente accede con privilegi elevati. Su windows, un evento 4672 viene prima di un evento 4624, se così non dovesse essere, potrebbe essere un sintomo di una manipolazione dei log di sistema.
Viene specificato:
Privileges Assigned: elenca i privilegi assegnati all'utente
Account Name: nome dell'account amministrativo

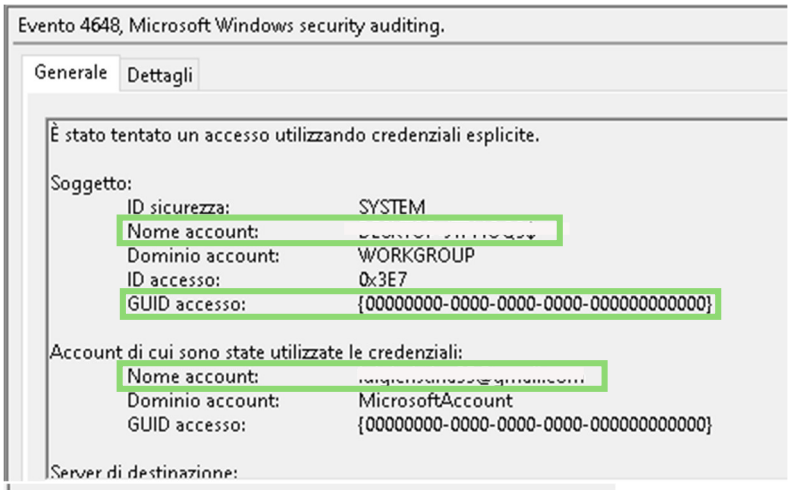


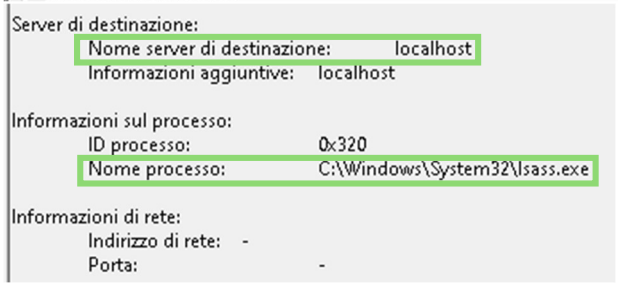
ID 4648

viene registrato quando un processo utilizza credenziali esplicite per autenticarsi su un sistema.



Account Name: L'account che ha avviato il processo che usa credenziali diverse.
Logon GUID: Identificativo univoco della sessione di logon.
Process Name: il processo che ha usato le credenziali (es. runas.exe, mstsc.exe, powershell.exe).
Account Whose Credentials Were Used: Il nome utente e il dominio delle credenziali inserite.
Target Server Name: Il nome del server o sistema di destinazione.
Source Network Address: L'IP da cui è stato effettuato il logon.
Logon Type: Il tipo di logon (vedi tabella pagina successiva).





Logon Type	Descrizione	Esempi D'uso
2	Interactive	Login con tastiera/mouse
3	Network	Accesso a una risorsa di rete
9	NewCredentials	Login con credenziali diverse da quelle attuali
10	Remoteinteractive	Accesso Desktop Remoto (RDP)