S9-E4 Umberto Valentini

FILE DI LOG DI WINDOWS

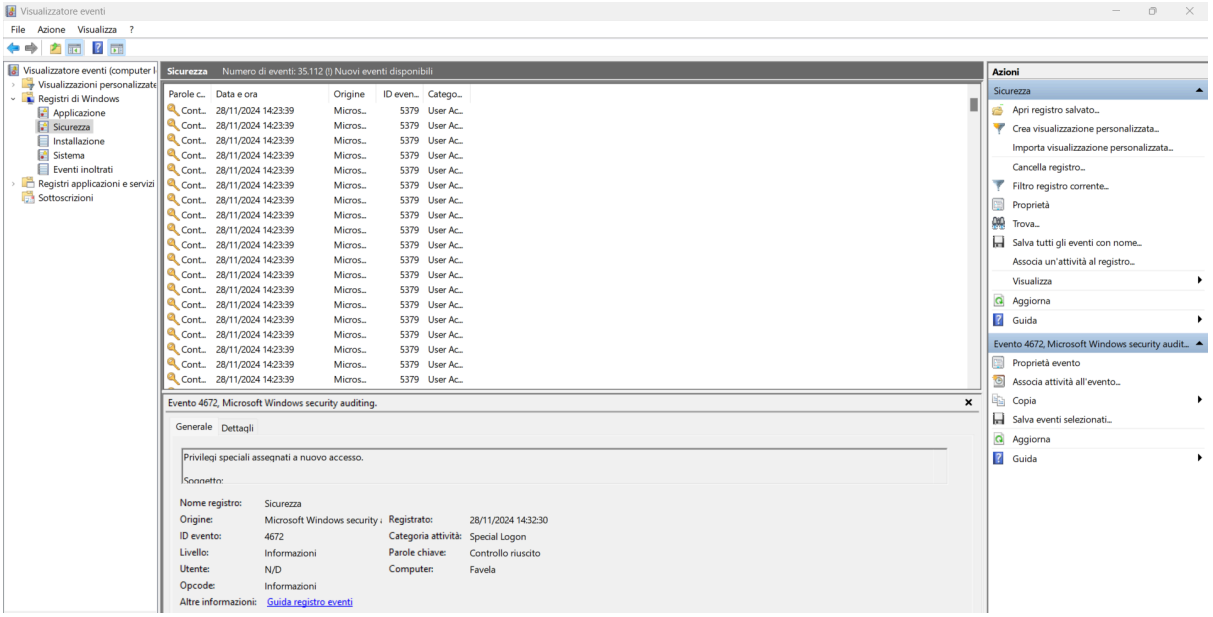
Il *System Log* (o syslog) è un registro in cui vengono raccolti messaggi e notifiche generate da vari componenti del sistema operativo, applicazioni e dispositivi hardware. È uno strumento fondamentale per monitorare l'attività di un sistema, identificare anomalie e diagnosticare problemi di funzionamento.

Definizione e Utilizzo

Il system log contiene informazioni dettagliate su eventi di sistema come errori, avvisi, accessi, operazioni di rete e attività dei processi. Questi dati, solitamente organizzati in ordine cronologico, offrono una panoramica completa dello stato e delle attività di un sistema. L'analisi dei log è principalmente una funzione svolta dal Livello 1 e dal Livello 2 del SOC, con una certa interazione anche dal Livello 3 in caso di incidenti complessi. Nel contesto di un Security Operations Center (SOC), i system log sono una risorsa cruciale per:

1. **Monitoraggio continuo:** Identificare comportamenti anomali o indicatori di compromissione (IOC).
2. **Analisi degli incidenti:** Ricostruire gli eventi in seguito a un attacco informatico.
3. **Conformità normativa:** Garantire che le operazioni rispettino standard di sicurezza e leggi in vigore.
4. **Automazione:** Alimentare sistemi SIEM (Security Information and Event Management) per correlare eventi e generare allarmi in tempo reale.

L'analisi dei system log richiede competenze specifiche e l'utilizzo di strumenti adeguati, ma rappresenta una delle attività fondamentali per garantire la sicurezza e la resilienza delle infrastrutture IT. La gestione efficace dei log è una delle prime linee di difesa contro le minacce informatiche.



Fondamentale è la possibilità di applicare un filtro, ciò non solo rende la ricerca più specifica, ma dimostra al contempo come ci sia una classificazione di tipologia di evento all'interno del registro.