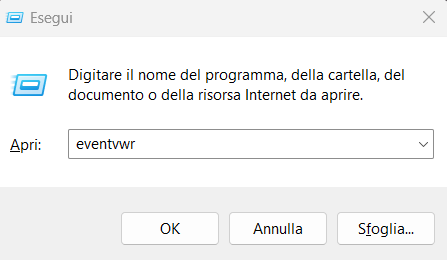
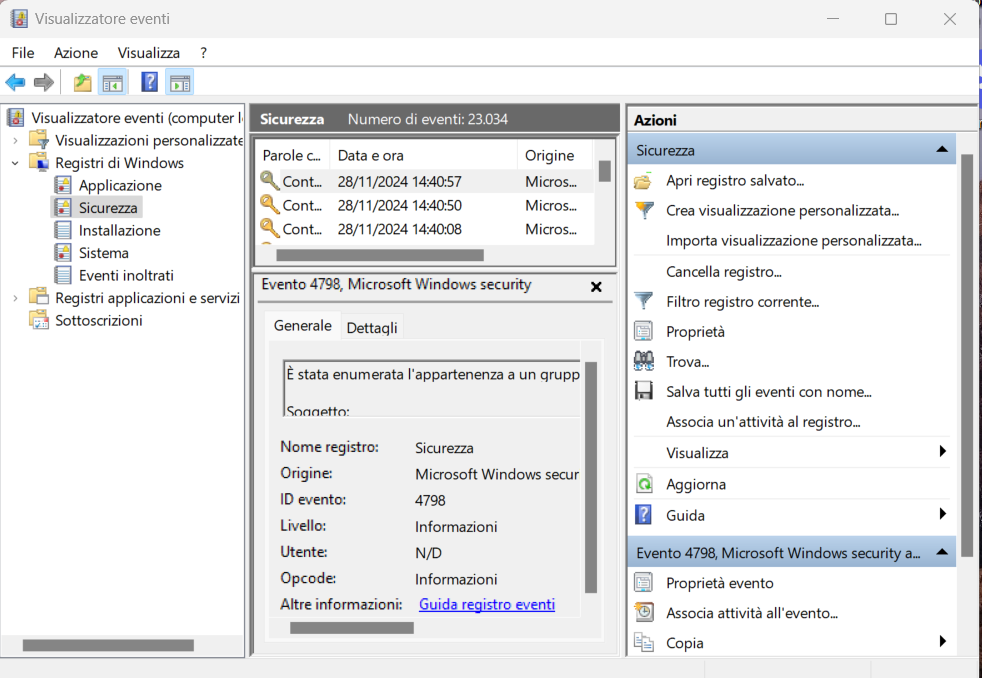
COMPITO S9L4

L’argomento di oggi è stato il SOC (Security Operations Center) e abbiamo discusso l’importanza dei file di log per il monitoraggio continuo degli eventi e per la raccolta di informazioni. I file di log rappresentano una risorsa fondamentale per rilevare anomalie, individuare potenziali minacce e garantire una risposta rapida e accurata agli incidenti di sicurezza.

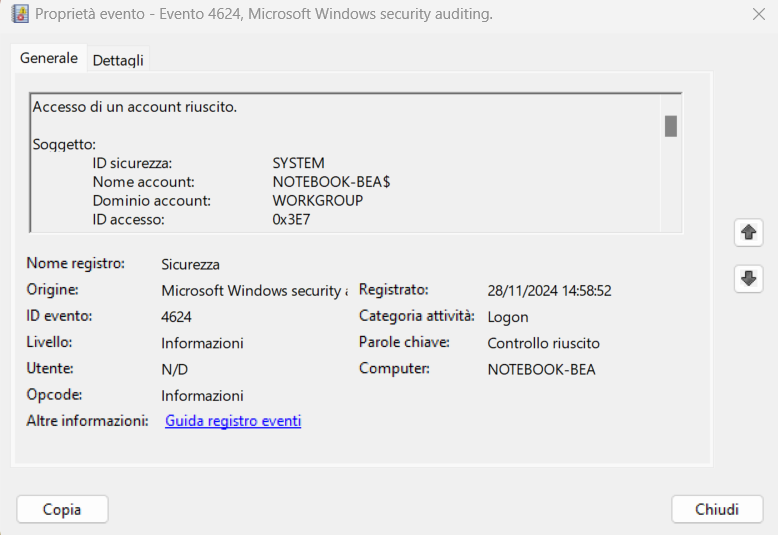
Per questo motivo la traccia di oggi prevedeva di gestire i file di log della sicurezza utilizzando il Visualizzatore eventi di Windows.



Come prima cosa abbiamo aperto il visualizzatore eventi di windows usando la combinazione di tasti **Win + r**; una volta aperta la finestra sulla sinistra abbiamo inserito il comando che si vede in figura



Si aprirà la finestra del visualizzatore eventi dove andremo nella parte relativa ai registri di windows ed entreremo nella sezione dedicata alla sicurezza, che ci mostrerà tutti i file di log relativi a questo argomento specifico



Quello che si vede in figura è un esempio di file di log tipico, presente all’interno della sezione sicurezza dei registri di windows e ci mostra l’accesso di un account riuscito con successo.

All’interno di un team operativo che si occupa di sicurezza sui sistemi informatici, come il SOC, è di fondamentale importanza l’analisi de dati. I file di log sono la prima fonte di dati che vengono raccolti nella SIEM per poi essere configurati, analizzati e classificati in base a dei livelli, che aiutano l’analista a capire quale anomalia ha un maggiore livello di criticità e quindi su quale agire in maniera più tempestiva per limitare i danni che quella minaccia può riportare all’azienda.

Quindi una buona raccolta dati è fondamentale per mitigare ed essere in grado di rispondere tempestivamente a delle minacce cercando di mantenere l’operatività dell’azienda o quantomeno ripristinarla nel minor tempo possibile per limitare l’impatto della minaccia sull’azienda stessa