# File di Log di Windows

## Introduzione

Il Visualizzatore eventi di Windows è uno strumento fondamentale per monitorare l'attività di sistema e individuare potenziali minacce alla sicurezza. Questo strumento registra una vasta gamma di eventi, tra cui errori, avvisi e informazioni dettagliate sulle attività di sistema. In questa relazione, ci concentreremo sulla configurazione e gestione specifica del registro di sicurezza, un componente cruciale per la protezione dei sistemi.

## Obiettivo

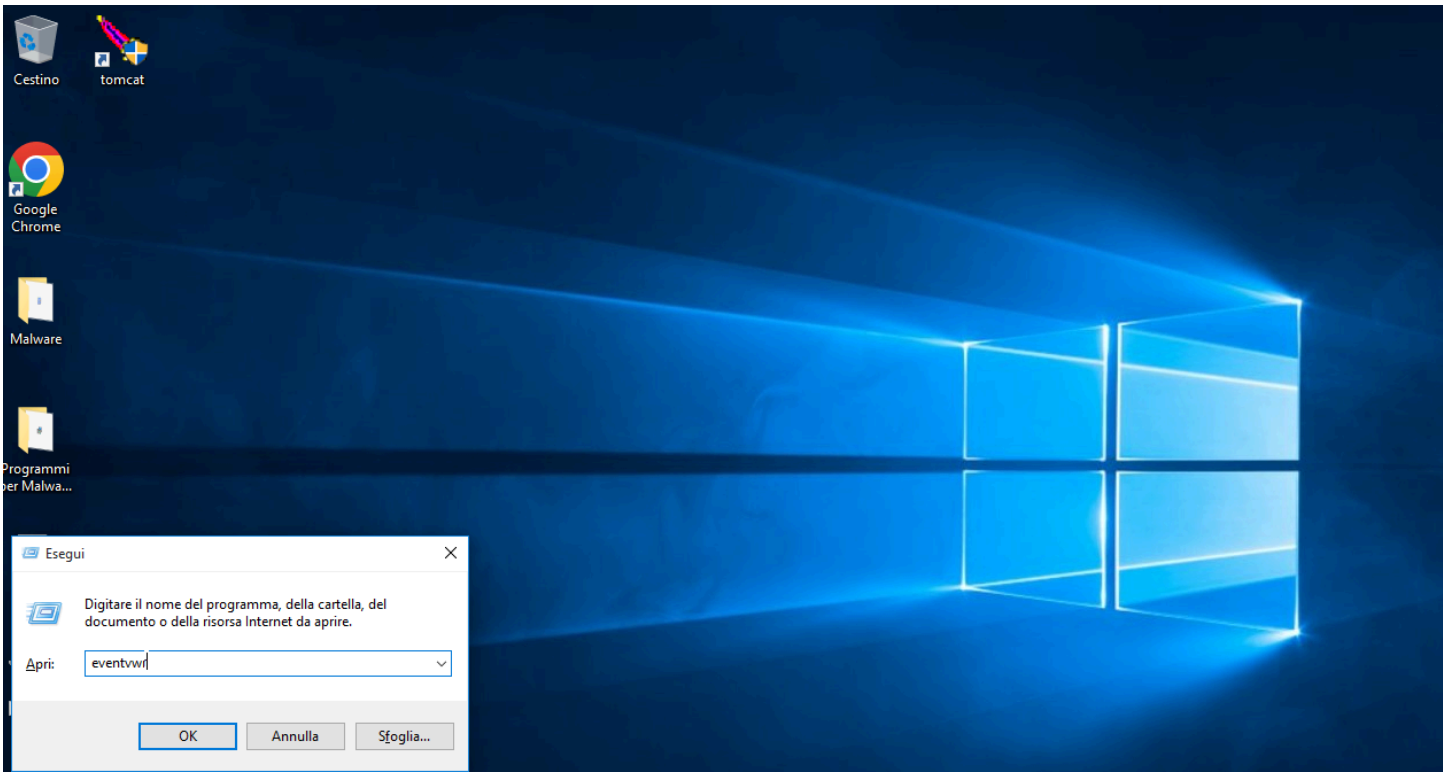
L'obiettivo principale di questa configurazione è garantire una corretta raccolta, archiviazione e analisi dei dati relativi agli eventi di sicurezza. Ciò permette di:

- **Identificare attacchi e intrusioni:** Monitorando le attività sospette e le modifiche non autorizzate alle risorse di sistema.
- **Risolvere problemi:** Analizzando i log per individuare le cause di malfunzionamenti e errori.
- **Conformarsi a normative:** Mantenendo una documentazione dettagliata delle attività di sistema per soddisfare i requisiti di conformità.

## Procedura

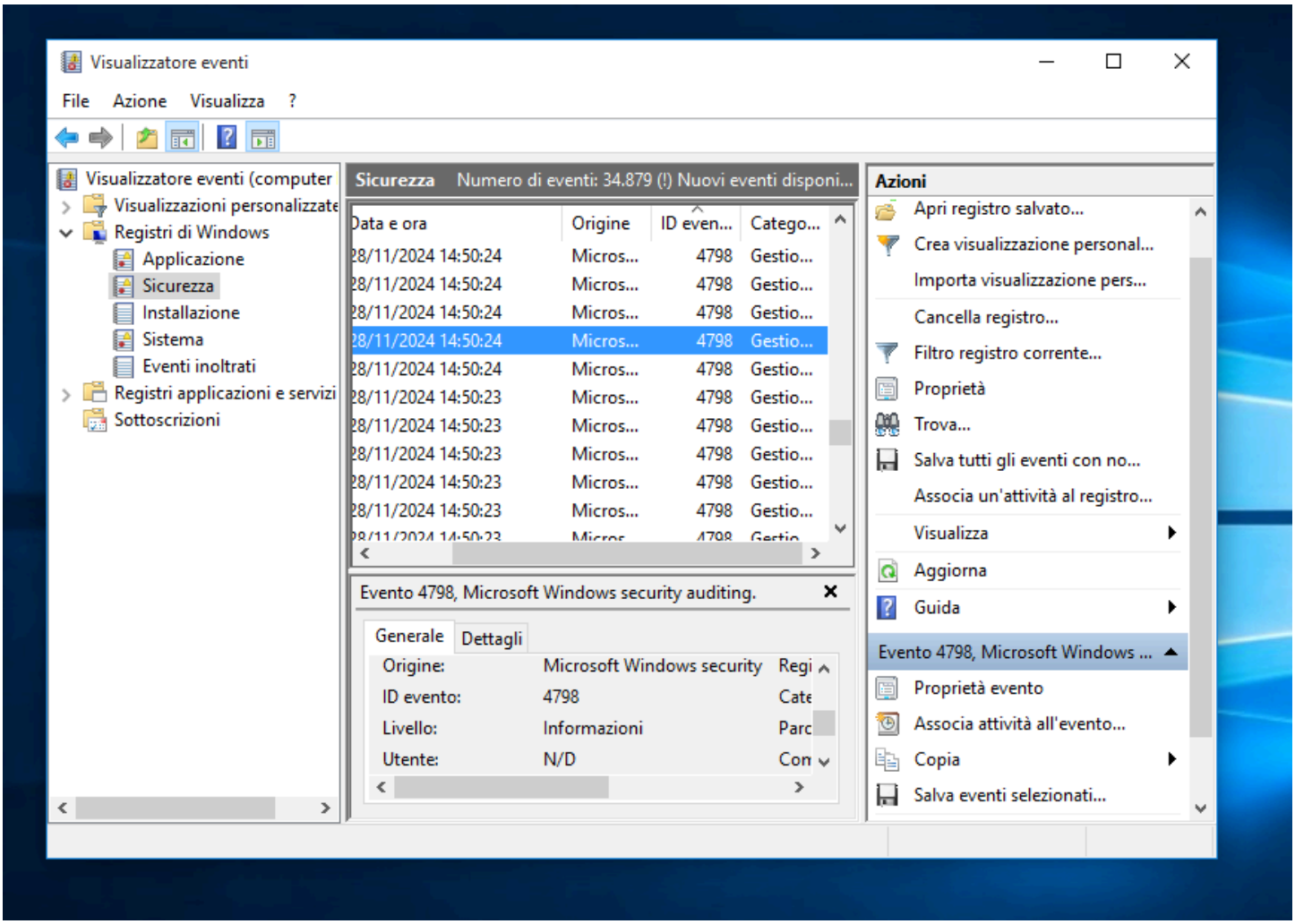
1. Accesso al Visualizzatore Eventi

- **Avvio rapido:** Premere contemporaneamente i tasti Windows + R per aprire la finestra "Esegui".
- **Comando:** Digitare "eventvwr" nella finestra "Esegui" e premere Invio. Si aprirà il Visualizzatore eventi.




## Configurazione delle Proprietà del Registro di Sicurezza

- **Navigazione:** Nel pannello di sinistra del Visualizzatore eventi, espandere "Registri di Windows" e selezionare "Sicurezza".
- **Proprietà:** Fare clic con il pulsante destro del mouse sul registro "Sicurezza" e selezionare "Proprietà".




## Informazioni Aggiuntive

- **Tipi di eventi:** Il registro di sicurezza registra una vasta gamma di eventi, tra cui:
  - **Accesso riuscito e non riuscito:** Tentativi di accesso a risorse di sistema.
  - **Modifiche alle autorizzazioni:** Modifiche ai diritti di accesso alle risorse.
  - **Eventi di sistema:** Avvio, arresto e riavvio del sistema.
  - **Eventi di sicurezza:** Attività legate alla sicurezza, come la creazione di nuovi account utente.
- **Analisi dei log:** Per analizzare efficacemente i log di sicurezza, è possibile utilizzare strumenti di analisi specializzati o scrivere script personalizzati.
- **Archiviazione dei log:** È consigliabile archiviare i log di sicurezza in modo sicuro per consentirne la consultazione futura in caso di indagini.
- **Sicurezza dei log:** È importante proteggere i log di sicurezza da accessi non autorizzati, implementando misure di controllo degli accessi e crittografando i dati.

## Conclusioni

La configurazione e la gestione corretta dei log di sicurezza sono fondamentali per garantire la sicurezza di un sistema informatico. Il Visualizzatore eventi di Windows offre un'interfaccia

intuitiva per monitorare e analizzare gli eventi di sicurezza. Seguendo i passaggi descritti in questa relazione, è possibile ottenere una visibilità completa sull'attività del sistema e identificare tempestivamente eventuali minacce.