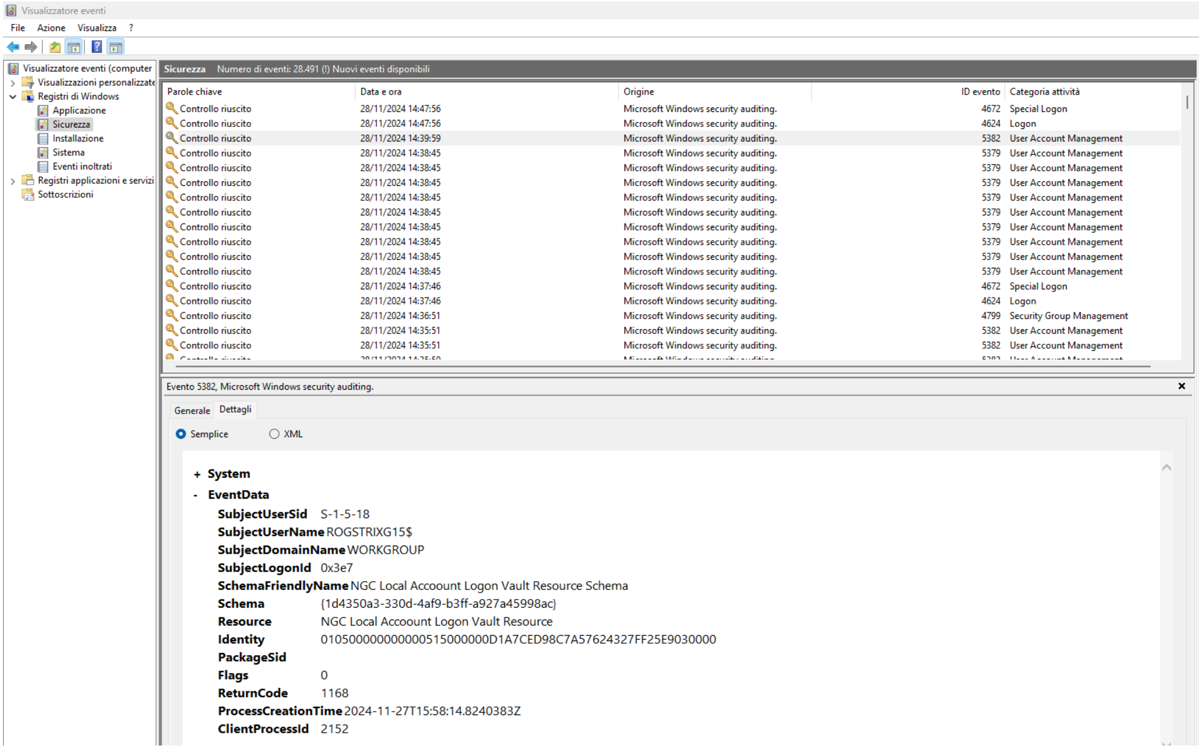
FILE DI LOG DI WINDOWS

Utilità della Pagina Sicurezza nei Registri di Windows

La sezione *Sicurezza* del Visualizzatore Eventi è uno strumento fondamentale per:

1. **Monitoraggio degli Accessi:**
   - Tracciare login riusciti e tentativi falliti.
   - Identificare modifiche significative agli account utente o alle impostazioni di sicurezza.
2. **Audit e Analisi di Incidenti:**
   - Rilevare attività sospette, come tentativi di accesso non autorizzati o manipolazioni dei privilegi.
3. **Conformità e Reporting:**
   - Generare log per dimostrare la conformità a normative di sicurezza o policy aziendali.
4. **Risoluzione dei Problemi:**
   - Fornire informazioni dettagliate su errori o anomalie legate alla sicurezza del sistema.

Esempio



Sicurezza Numero di eventi: 28.491 (!) Nuovi eventi disponibili

Parole chiave	Data e ora	Origine	ID evento	Categoria attività
Controllo riuscito	28/11/2024 14:47:56	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	28/11/2024 14:47:56	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	28/11/2024 14:39:59	Microsoft Windows security auditing.	5382	User Account Management
Controllo riuscito	28/11/2024 14:38:45	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	28/11/2024 14:38:45	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	28/11/2024 14:38:45	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	28/11/2024 14:38:45	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	28/11/2024 14:38:45	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	28/11/2024 14:38:45	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	28/11/2024 14:38:45	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	28/11/2024 14:38:45	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	28/11/2024 14:38:45	Microsoft Windows security auditing.	5379	User Account Management
Controllo riuscito	28/11/2024 14:37:46	Microsoft Windows security auditing.	4672	Special Logon
Controllo riuscito	28/11/2024 14:37:46	Microsoft Windows security auditing.	4624	Logon
Controllo riuscito	28/11/2024 14:36:51	Microsoft Windows security auditing.	4799	Security Group Management
Controllo riuscito	28/11/2024 14:35:51	Microsoft Windows security auditing.	5382	User Account Management
Controllo riuscito	28/11/2024 14:35:51	Microsoft Windows security auditing.	5382	User Account Management

Evento 5382, Microsoft Windows security auditing.

● Semplice ○ XML

```
+ System
- EventData
    SubjectUserSid        S-1-5-18
    SubjectUserName       ROGSTRIXG15$
    SubjectDomainName     WORKGROUP
    SubjectLogonId        0x3e7
    SchemaFriendlyName    NGC Local Accoount Logon Vault Resource Schema
    Schema                {1d4350a3-330d-4af9-b3ff-a927a45998ac}
    Resource              NGC Local Accoount Logon Vault Resource
    Identity              0105000000000005150000000D1A7CED98C7A57624327FF25E9030000
    PackageSid
    Flags                 0
    ReturnCode            1168
    ProcessCreationTime   2024-11-27T15:58:14.8240383Z
    ClientProcessId       2152
```

Possiamo osservare le seguenti informazioni:

1. **Elenco Eventi di Sicurezza:**
    - Gli eventi sono organizzati per data e ora, con una colonna dedicata all'ID evento (es. 4672, 5382, ecc.) e alla relativa categoria di attività (es. *Special Logon*, *User Account Management*).
    - L'origine di questi eventi è indicata come *Microsoft Windows Security Auditing*.
2. **Dettagli di un Evento Specifico (ID Evento 5382):**
    - **Nome Schema:** "NGC Local Account Logon Vault Resource Schema".
    - **User SID e Nome Utente:** L'utente coinvolto è identificato come "ROGSTRIXG15$" con SID "S-1-5-18".
    - **Risorsa Accessibile:** L'evento riguarda un accesso al vault locale delle credenziali.
    - **Timestamp:** L'evento è stato generato il 27 novembre 2024 alle 15:58.

Conclusioni

La configurazione e la gestione dei registri di sicurezza in Windows consentono di rafforzare la protezione del sistema, fornendo una traccia chiara di tutte le attività.

Durante l'esercizio, abbiamo appreso come accedere ai log e analizzare i dettagli per migliorare la sicurezza.