Relazione sull'analisi degli eventi di sicurezza con Splunk

Cos'è Splunk e a cosa serve?

Splunk è una piattaforma di analisi dei dati utilizzata per **raccogliere, indicizzare e visualizzare informazioni** provenienti da diverse fonti, come log di sistema, applicazioni, dispositivi di rete e altro.

Questo software permette di:

- rilevare e rispondere rapidamente alle minacce
- automatizzare i processi di monitoraggio e analisi dei log, riducendo il carico di lavoro manuale.
- analizzare e filtrare grandi quantità di dati per fornire insight dettagliati e basati su prove

Vantaggi per il SOC (Security Operations Center)

1. **Monitoraggio in tempo reale:** consente di individuare attività sospette o violazioni di sicurezza immediatamente.
2. **Automazione:** permette di impostare avvisi automatici per eventi critici.
3. **Ricerca avanzata:** grazie alle query, il SOC può analizzare e correlare grandi volumi di dati rapidamente.
4. **Dashboard personalizzate:** fornisce report e visualizzazioni utili per prendere decisioni rapide e informate.
5. **Riduzione dei tempi di risposta:** migliora l'efficienza nella gestione degli incidenti di sicurezza.

Configurazione macchine

Server

- **Sistema operativo**: Windows Server 2022
- **IP**: `192.168.1.23`
- **Porta di ascolto**: `9997`

Client

- **Sistema operativo**: Windows 10 Pro 22h2
- **IP**: `192.168.1.24`
- **Porta di invio**: `9997`

Descrizione della query

Prendiamo in analisi un evento di sicurezza avvenuto nella macchina client.

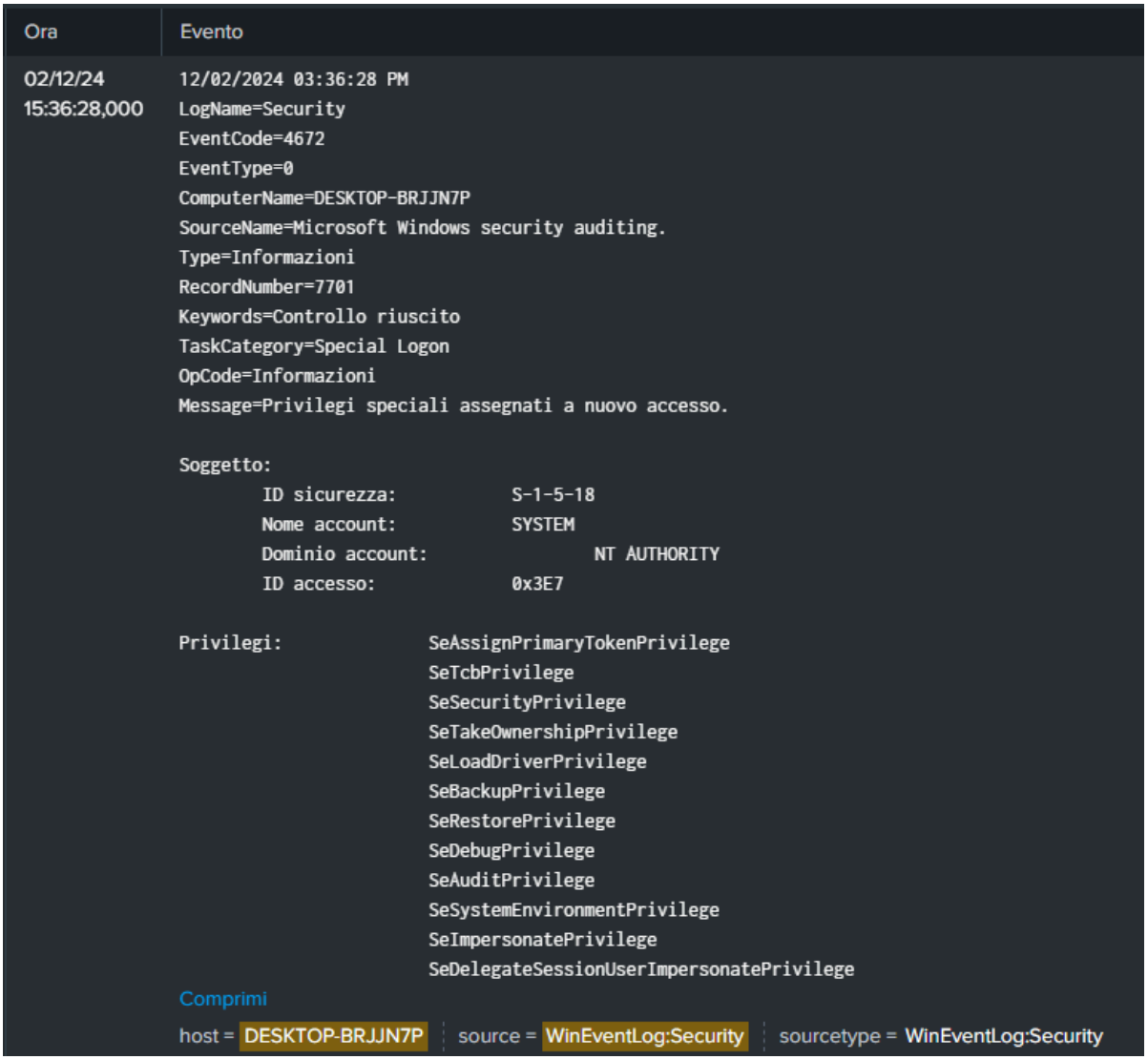
La query utilizzata è: `source="WinEventLog:Security" host="DESKTOP-BRJJN7P"`

Significato:

- `source="WinEventLog:Security"`
  - filtra gli eventi provenienti dal registro di sicurezza di Windows.
- `host="DESKTOP-BRJJN7P"`
  - restringe i risultati agli eventi generati dal computer specifico identificato come "DESKTOP-BRJJN7P".

Questa query serve a individuare eventi di sicurezza (come accessi, modifiche ai privilegi, ecc.) relativi a un host specifico.

Analisi dell'evento



Evento identificato:

- **Codice evento:** 4672
- **Descrizione:** "Privilegi speciali assegnati a nuovo accesso."
- **Spiegazione**: Questo evento viene generato ogni volta che un account effettua un logon ed è associato a privilegi amministrativi avanzati.

Dettagli rilevanti:

- **Utente:** SYSTEM (account con privilegi estremi, operante sotto NT AUTHORITY).
- **Privilegi assegnati:** Tra i privilegi elencati troviamo:
    - `SeTakeOwnershipPrivilege`: consente di assumere la proprietà di oggetti (es. file e processi), potenzialmente pericoloso.

    - `SeDebugPrivilege`: permette di accedere a processi di altri utenti, spesso utilizzato da malware per eseguire codice arbitrario.
    - `SeBackupPrivilege` e `SeRestorePrivilege`: consentono accesso illimitato ai file, bypassando i permessi.
    - Altri privilegi elevati che garantiscono controllo completo sul sistema.

Valutazione della pericolosità:

- **Non sempre pericoloso:** Questo evento è normale per account di sistema come SYSTEM, che richiedono privilegi avanzati per eseguire operazioni critiche. In genere si vedono molti di questi eventi nel registro eventi, perché ogni accesso all'account SYSTEM (Sistema locale) attiva questo evento.
- **Potenziale rischio:** Se l'evento è associato a un account utente non autorizzato o a un processo sconosciuto, potrebbe indicare un'escalation di privilegi da parte di un attaccante.

Conclusioni

- **Utilità di Splunk:** La piattaforma si dimostra essenziale per rilevare eventi di sicurezza e distinguere attività legittime da possibili minacce.
- **Evento analizzato:** Nel caso specifico, l'evento 4672 non è intrinsecamente pericoloso poiché coinvolge l'account SYSTEM, ma richiede monitoraggio per assicurarsi che non venga abusato.
- **Raccomandazioni:** È opportuno:
    1. Configurare avvisi per monitorare escalation di privilegi non autorizzate.
    2. Correlare questo evento con altri per rilevare attività sospette (ad esempio, accessi remoti imprevisti o modifica di impostazioni di sicurezza).

Splunk rappresenta uno strumento indispensabile per i SOC, garantendo una maggiore consapevolezza situazionale e riducendo il tempo necessario per individuare e rispondere a potenziali minacce.