Consegna S9-L4

Consegna: Creazione e Gestione delle Regole per i File di Log della Sicurezza in Windows

⚜️ **Tag:** #windows #visualizzatore_eventi #log_sicurezza #configurazione

Obiettivo

Configurare e gestire i file di log della sicurezza utilizzando il **Visualizzatore eventi** di Windows.

Istruzioni

1. **Accedere al Visualizzatore Eventi:**
   - Aprire il Visualizzatore eventi premendo **Win + R** per aprire la finestra "Esegui".
   - Digitare `eventvwr` e premere Invio.
2. **Configurare le Proprietà del Registro di Sicurezza:**
   - Nel pannello di sinistra, espandere "Registri di Windows" e selezionare "Sicurezza".
   - Fare clic con il tasto destro su "Sicurezza" e scegliere **Proprietà**.
   - Configurare:
     - **Dimensione massima del registro:** Specificare un valore adeguato in base alle politiche aziendali.
     - **Opzioni di sovrascrittura:** Selezionare tra:
       - Sovrascrivere gli eventi più vecchi.
       - Non sovrascrivere eventi.

    - Sovrascrivere eventi più vecchi di un determinato numero di giorni.
3. **Impostare un Filtro per il Registro Corrente:**
    - Fare clic con il tasto destro su "Sicurezza" e selezionare **Filtro registro corrente**.
    - Specificare gli ID degli eventi da monitorare (es. accesso, modifiche ai file, ecc.).
    - Applicare e salvare il filtro.
4. **Esportare i File di Log:**
    - Fare clic con il tasto destro su "Sicurezza" e selezionare **Salva eventi con nome**.
    - Salvare il file in formato **.evtx** per l'analisi futura.
5. **Verifica della Configurazione:**
    - Eseguire un test generando un evento (es. accesso fallito) e controllare che sia registrato.
    - Assicurarsi che le impostazioni siano persistenti dopo un riavvio del sistema.

Conclusione

Questa esercitazione consente di comprendere come configurare, gestire e monitorare i registri di sicurezza di Windows, un passaggio essenziale per la gestione della sicurezza aziendale.

🔑 **Chiavi:**
[windows, visualizzatore_eventi, log_sicurezza, configurazione]